10x Zoom · Dual Streams · PoE **PZ7111/PZ7112/PZ7121/PZ7122**

NETWORK CAMERA

User's Manual



VIVOTEK
www.vivotek.com

IP Surveillance

Table of Contents

Overview....................3
Read Before Use....................3
Package Contents....................3
Physical Description....................4
Installation....................7
Hardware Installation....................7
Network Deployment....................8
Software Installation....................11
Accessing the Network Camera....................12
Using Web Browsers....................12
Using RTSP Players....................14
Using 3GPP-compatible Mobile Devices....................15
Using VIVOTEK Recording Software....................16
Main Page....................17
Client Settings....................21
Configuration....................23
System....................24
Security....................26
HTTPS....................27
Network....................32
Wireless LAN (PZ7112/PZ7122 only)....................43
DDNS....................46
Access List....................48
Audio and Video....................51
Motion Detection....................57
Camera Control....................59
Homepage Layout....................62
Application....................65
Recording....................78
System Log....................81
View Parameters....................82
Maintenance....................83
Appendix....................87
URL Commands for the Network Camera....................87
Technical Specifications....................124
Technology License Notice....................125
Electromagnetic Compatibility (EMC)....................126

Overview

VIVOTEK's PZ71x1(PoE)/71x2(WLAN) is a high-performance network camera featuring 10x zoom and pan/tilt functionality. The camera is designed for indoor surveillance applications such as retail stores, offices, and banks.

The built-in 10x motorized optical zoom module provides excellent depth of field when zoomed in, displaying clear-cut images of near or distant objects. With 300-degree pan and 135-degree tilt, the camera can achieve a wide range of view, giving users more comprehensive control over the monitored site. The PZ7111/7121 is incorporated with VIVOTEK's self-developed Bach SoC; therefore, users can benefit from the advantages of dual-codec video and two-way audio. With support for simultaneous dual streaming, the camera allows users to view MJPEG or MPEG-4 videos on multiple platforms such as web browsers or 3G cell phones.

VIVOTEK's PZ7111/7121 also supports wireless and Power-over-Ethernet connection, making installation easier and more cost-efficient. The free, standard, multi-lingual 16-channel recording software helps users to seamlessly set up an easy-to-use IP surveillance system.

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal and complies with all privacy laws before installing this unit for its intended use.
It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

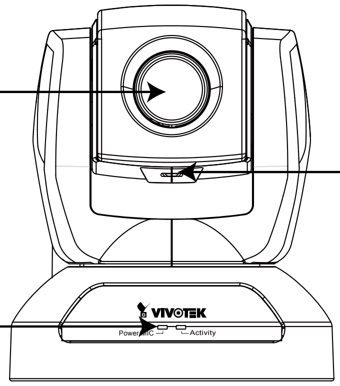
The Network Camera is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For more creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

Package Contents

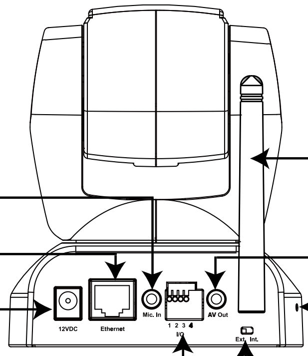
- PZ7111/PZ7112/PZ7121/PZ7122
- Power Adapter
- Antenna (PZ7112/PZ7122 only)
- Screws
- Quick Installation Guide
- Warranty Card
- Software CD
- A/V Cable
- Ceiling Mount Brackets

Physical Description

Front panel

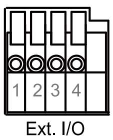


Rear panel



General I/O Terminal Block

This Network Camera provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below.

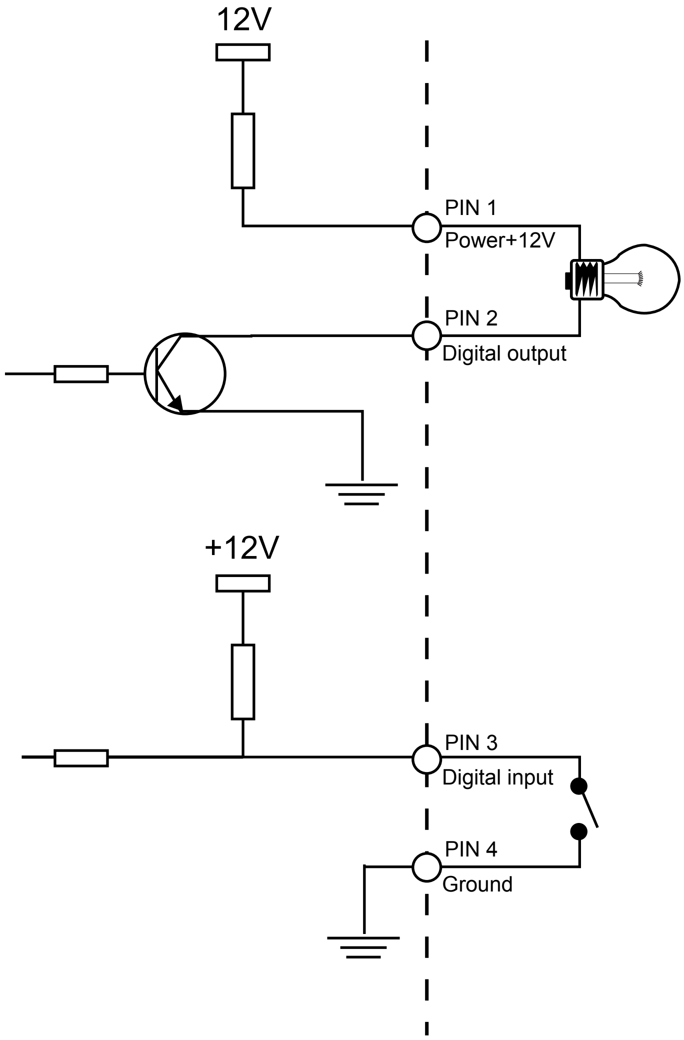


1: Power
2: Digital output
3: Digital input
4: Ground

Pin	Name	Specification	Remarks
1	Power	12VDC ± 5%, max. 1.5A	Max. rating 2A
2	Digital output	Max. 40VDC, max. 400mA, isolation 2kV	
3	Digital input	OPEN/Short-to-GND, isolation 2kV	Internal pull-up
4	Ground		

DI/DO Diagram

Please refer to the following illustration for the connection method.

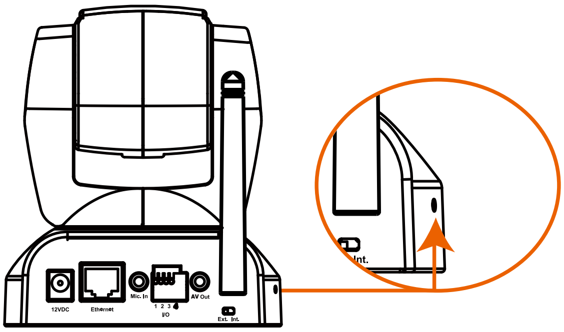


Status LED

The color of LED indicates the status of the Network Camera.

Status LED Color	Description
Blinking red	Power is being supplied to the Network Camera.
Solid green	The Network Camera is booting up.
Steady green with blinking red	The Network Camera is trying to obtain an IP address.
Steady green and red	An IP address is successfully assigned to the Network Camera.
Steady red with blinking green	The Network Camera is working.
Blinking red and green	During firmware upgrade.

Hardware Reset



The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after rebooting, restore the factory settings and install again.

Reset: Press and release the recessed reset button with a paper clip or thin object. Wait for the Network Camera to reboot.

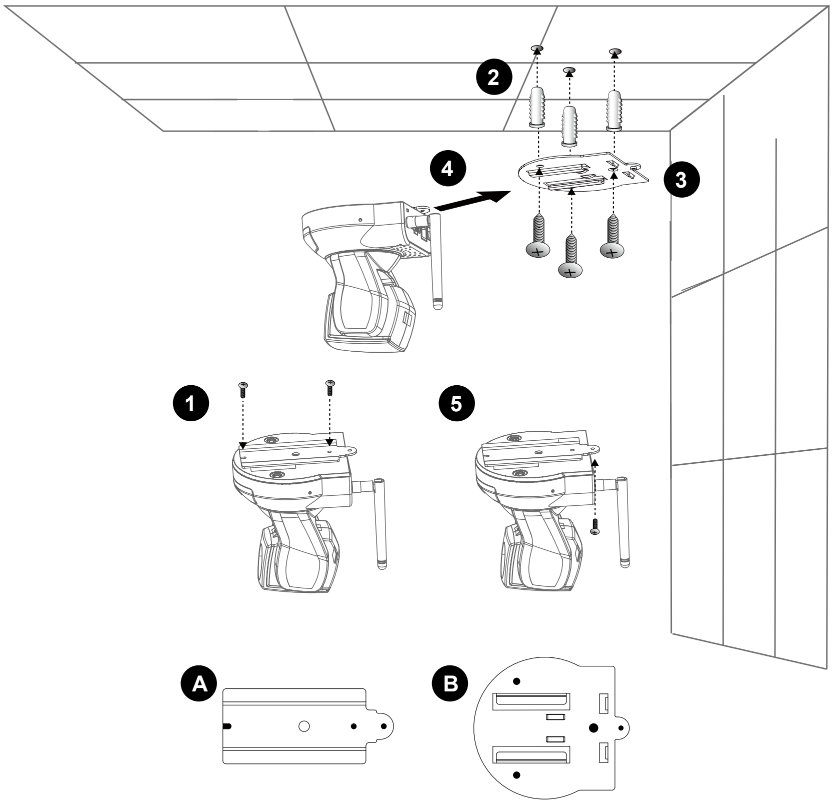
Restore: Press and hold the recessed reset button until the status LED rapidly blinks red and green simultaneously. Note that all settings will be restored to factory default.

Installation

Hardware Installation

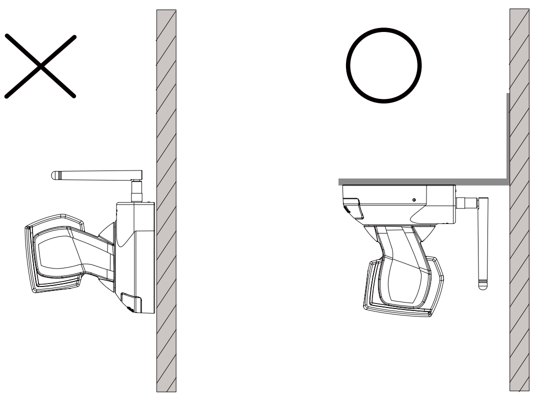
Follow the steps below to install the Network Camera to the ceiling:

1. Attach ceiling mount bracket A to the Network Camera and secure it with two small screws.
2. Drill three pilot holes into the ceiling; hammer the plastic anchors into the holes.
3. Fasten ceiling mount bracket B to the ceiling with three screws.
4. Slide the Network Camera into ceiling mount bracket B.
5. Secure the ceiling mount bracket A and B with a small screw.

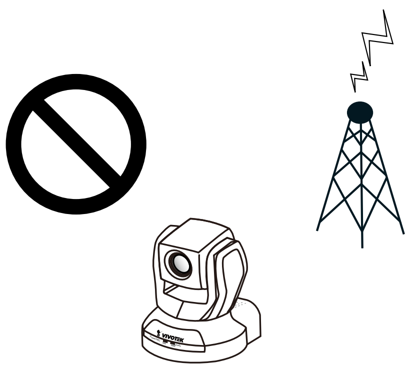


NOTE

► *If you want to intall the Network Camera on the wall, please use the wall mount bracket (optional, not included in the package).*



► *Keep away from interference source to make sure performance integrate, and avoid snow or moiré patterning.*

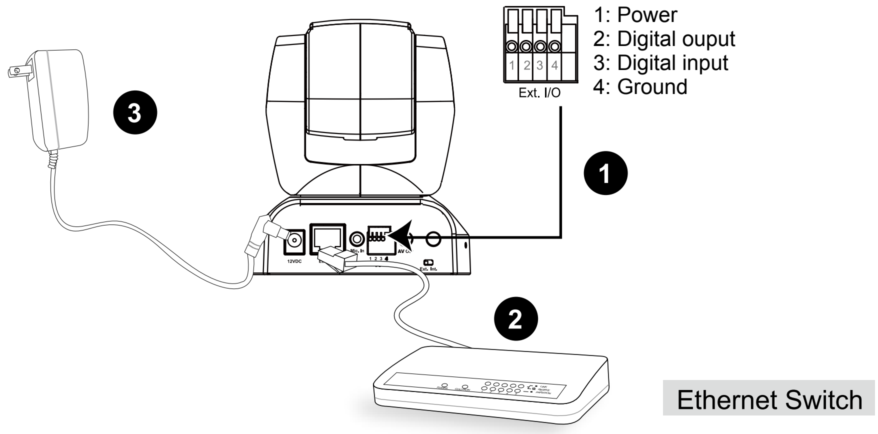


Network Deployment

Setup the Network Camera over the Internet

This section explains how to configure the Network Camera over an Internet connection.

1. If you have external devices such as sensors and alarms, connect them to the general I/O terminal block.
2. Connect the camera to a switch via Ethernet cable.
3. Connect the supplied power cable from the Network Camera to a power outlet.

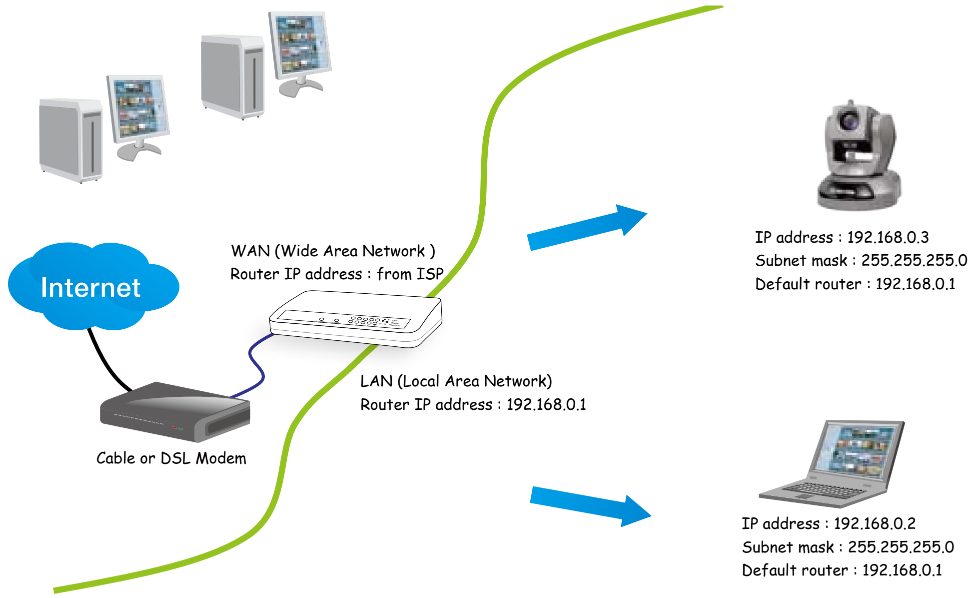


There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 11 for details.



2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

■ HTTP port
■ RTSP port
■ RTP port for audio
■ RTCP port for audio
■ RTP port for video
■ RTCP port for video

If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to your router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 32 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN on page 32 for details.

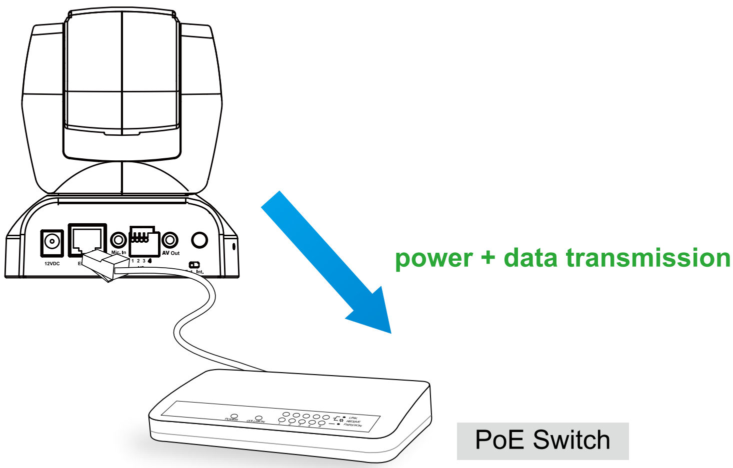
Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 33 for details.

Set up the Network Camera through Power over Ethernet (PoE) (PZ71x1 only)

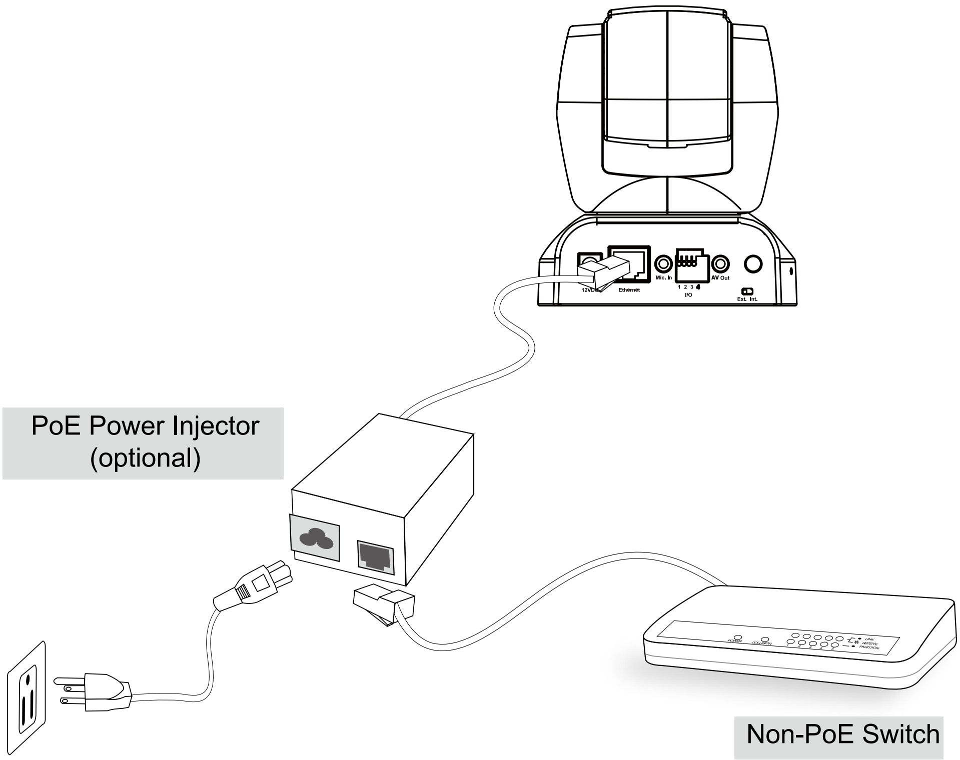
When using a PoE-enabled switch

The Network Camera is PoE-compliant, which allows it to be powered via a single Ethernet cable. If your switch/router supports PoE, refer to the following illustration to connect the Network Camera to a PoE-enabled switch/router.



When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch/router.



Software Installation

Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up your Network Camera on the LAN.

1. Install IW2 from the Software Utility directory on the software CD.
   Double click the IW2 shortcut on your desktop to launch the program.



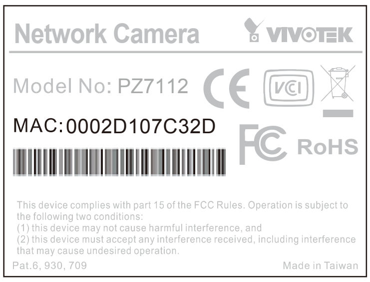
2. The program will conduct an analysis of your network environment.
   After your network environment is analyzed, please click **Next** to continue the program.





3. The program will search for all VIVOTEK network devices on the same LAN.

4. After searching, the main installer window will pop up. Click on the MAC and model name which matches the product label on your device to connect to the Network Camera via Internet Explorer.



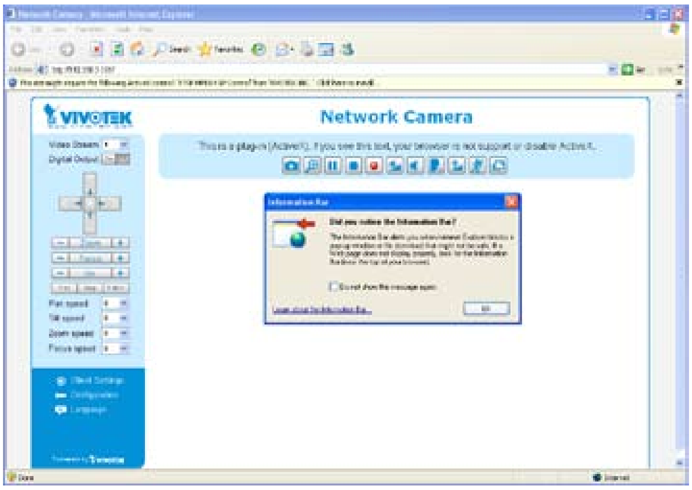


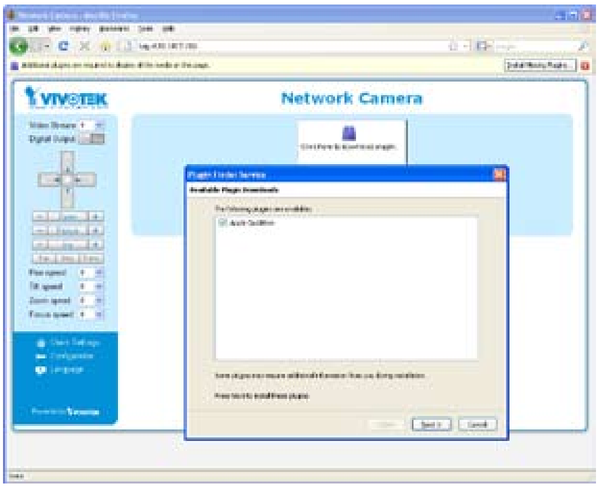
Accessing the Network Camera

This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

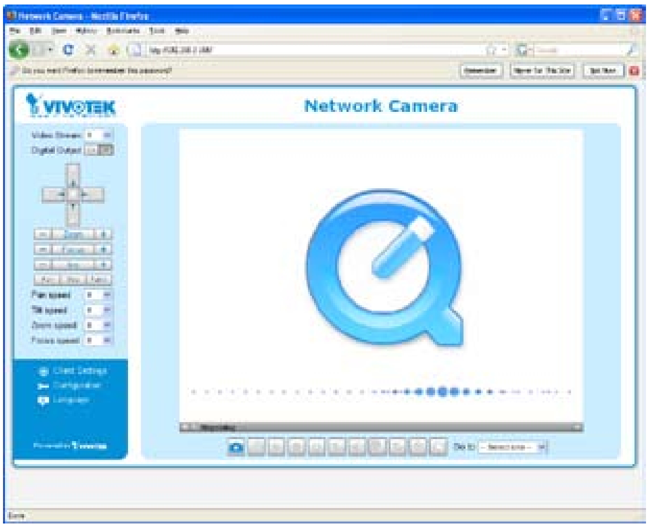
Use Installation Wizard 2 (IW2) to access to the Network Cameras installed on the LAN.
If your network environment is not the LAN, follow these steps to access the Network Camera:
1. Launch your web browser (eg. Microsoft® Internet Explorer, Mozilla Firefox, or Netscape).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If this is the first time installing the VIVOTEK network camera, an information bar will pop up as shown below. Follow the instructions to install the required plug-in on your computer.

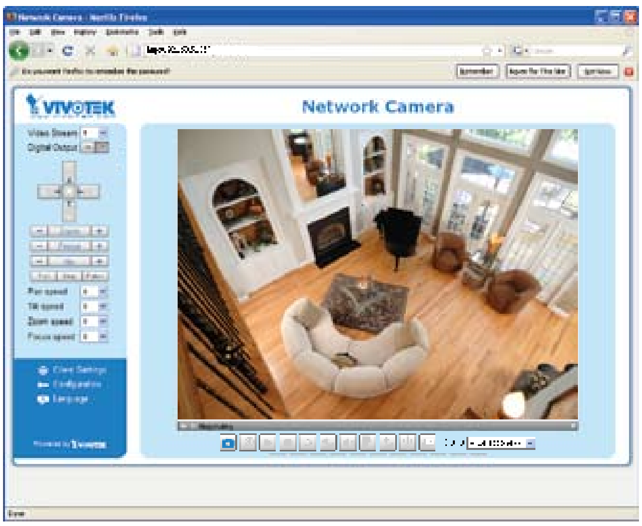




NOTE

► *For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you do not have Quick Time on your computer, please install it first, then launch the web browser.*

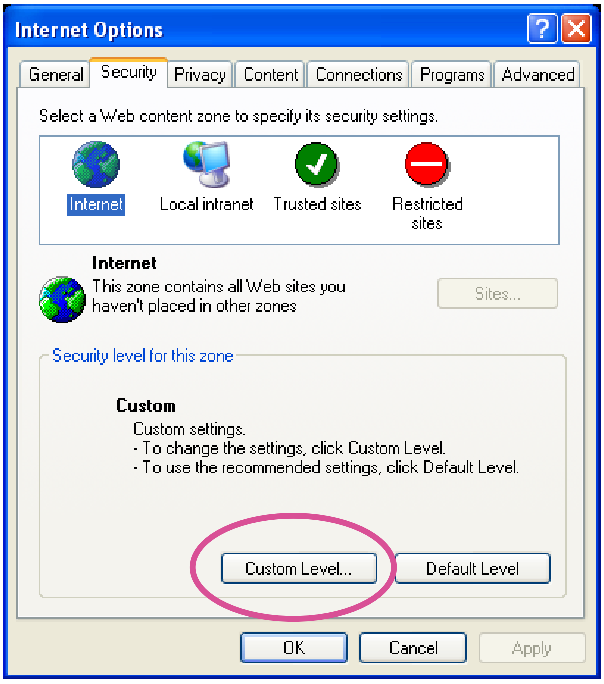




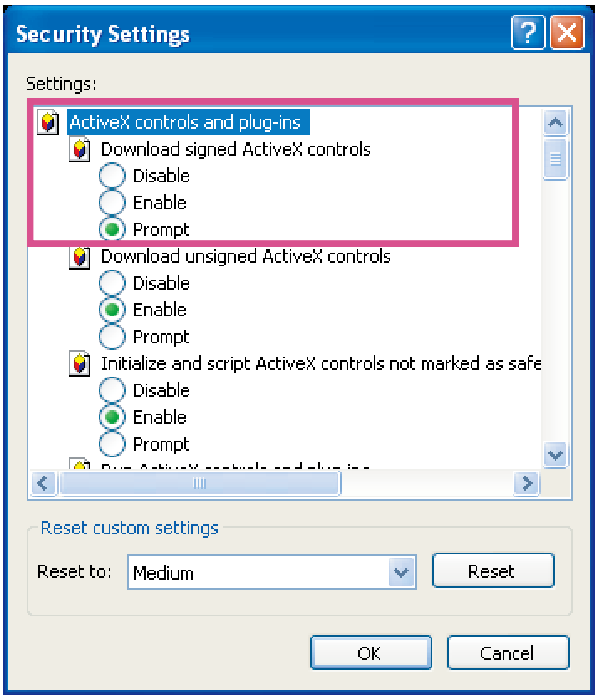
► *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera.*
For more information about how to enable password protection, please refer to Security on page 26.

► *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.*

1. Choose Tools > Internet Options > Security > Custom Level.



*2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.*



3. Refresh your web browser, then install the Active X® control. Follow the instructions to complete installation.

Using RTSP Players

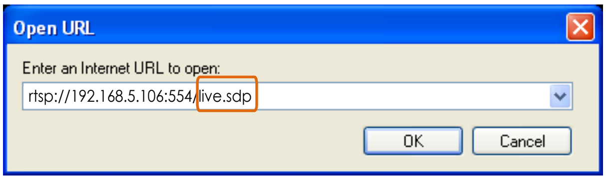
To view the MPEG-4 streaming media using RTSP players, you can use one of the following applications that support RTSP streaming.

Quick Time Player

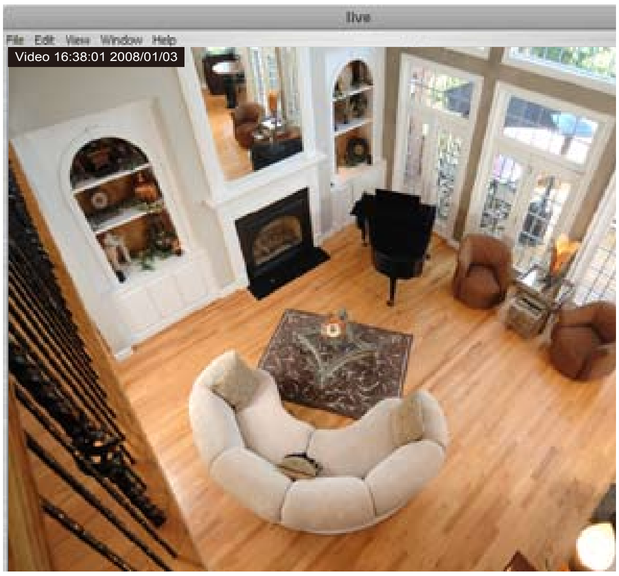
Real Player

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 41.
For example:



4. The live video will be displayed in your player.
   For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 41 for details.



Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 8.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 41.

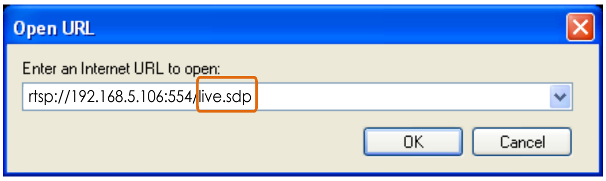
2. As the the bandwidth on 3G networks is limited, larger video sizes are not available. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Audio and Video on page 51.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (GSM-AMR)	12.2kbps

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 41.

4. Launch the players on 3GPP-compatible mobile devices (ex. Real Player).

5. Type the following URL commands in the player.
   The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>.
   For example:



Using VIVOTEK Recording Software

The product software CD also contains VIVOTEK's recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software, then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download the manual from http://www.vivotek.com.



Main Page

This chapter explains the layout of the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, PTZ Control Panel, Configuration Area, and Live video window.



VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

Host Name

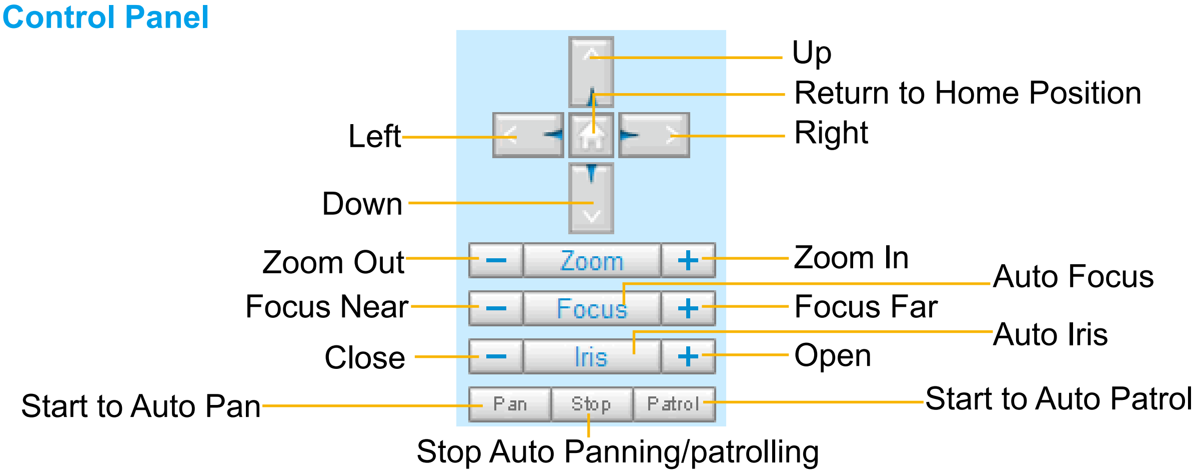
The host name can be customized to fit your needs. For more information, please refer to System on page 24.

Camera Control Area

Video Stream: This Network Camera supports MJPEG or MPEG-4 dual streams simultaneously. You can select either one for live viewing.

Digital Output: Click to turn the digital output device on or off.

PTZ Control Panel



Pan: Click this button to start the auto pan. When the current position is Home or on the left side of Home, the camera starts panning from the current position to the left-most position, then to the right-most position, and finally backward to the original position. When the current position is on the right side of Home, the camera starts panning from the current position to the right-most position, then to the left-most position, and finally backward to the original position.

Stop: Click this button to stop the Auto Pan and Auto Patrol functions.

Patrol: Once the Administrator has determined the list of preset positions, click this button to command the camera to patrol among those positions on the Patrol List. For more information, please refer to Camera Control on page 59.

Pan /Tilt /Zoom /Focus speed: Adjust the speed of pan/ tilt/ zoom/ focus.

Pan speed	Tilt speed	Zoom speed	Focus speed	
-5	-5	-5	-5	Slower
-4	-4	-4	-4	
-3	-3	-3	-3	
-2	-2	-2	-2	
-1	-1	-1	-1	
0	0	0	0	
1	1	1	1	
2	2	2	2	
3	3	3	3	
4	4	4	4	
5	5	5	5	Faster

Configuration Area

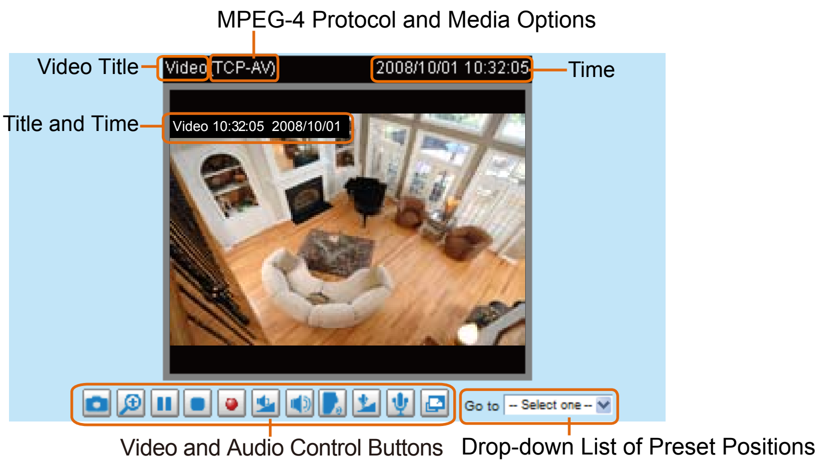
Client Settings: Click this button to access the client settings page. For more information, please refer to Client Settings on page 21.

Configuration: Click this button to access the configuration page of the Network Camera. It is suggested that a password be applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 23.

Language: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Live Video Window

■ The following window is displayed when the video mode is set to MPEG-4:



Video Title: The video title can be configured. For more information, please refer to Video Settings on page 51.

MPEG-4 Protocol and Media Options: The transmission protocol and media options for MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 21.

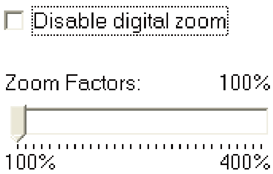
Time: Display the current time. For further configuration, please refer to Video Settings on page 51.

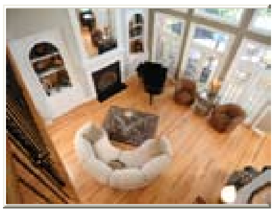
Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Video Settings on page 51.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen image.





Pause: Pause the transmission of the streaming media. The button becomes the Resume button after clicking the Pause button.

Stop: Stop the transmission of the streaming media. Click the Resume button to continue transmission.

Start MP4 Recording: Click this button to record video clips in MP4 file format. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on page 22 for details.

Volume: If the Mute function is not activated, move the slider bar to adjust the volume on the local computer.

Mute: Turn off the volume on the local computer. The button becomes the Audio On button after clicking the Mute button.

Talk: Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button again to end talking transmission.

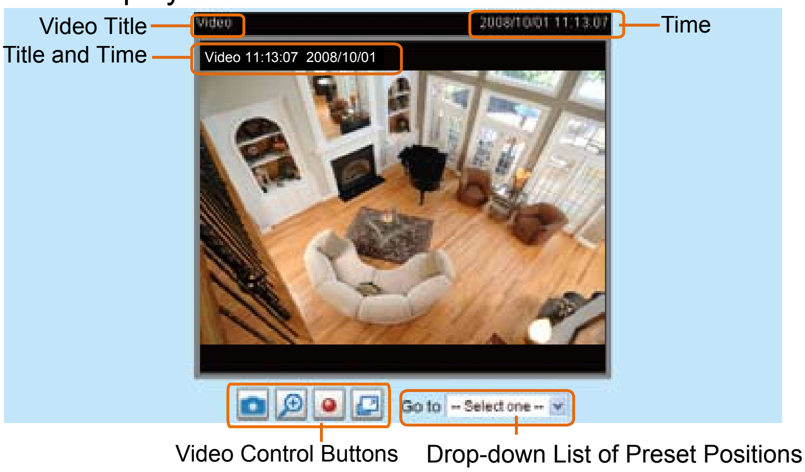
Mic Volume: When the Mute function is not activated, move the slider bar to adjust the microphone volume on the local computer.

Mute: Turn off the Mic volume at local computer. The button becomes the Mic On button after clicking the Mute button.

Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

Go to: Once the Administrator has determined the list of preset positions, you can aim the camera using this command. For more information, please refer to Camera Control on page 59.

■ The following window is displayed when the video mode is set to MJPEG:



Video Title: The video title can be configured. For more information, please refer to Video Settings on page 51.

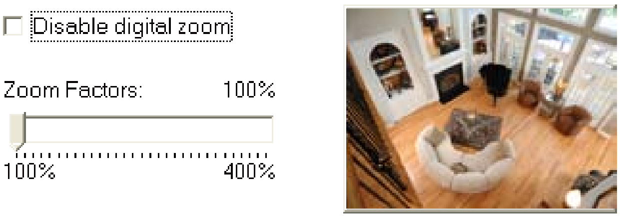
Time: Display the current time. For more information, please refer to Video Settings on page 51.

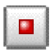
Title and Time: The video title and time can be stamped on the streaming video. For more information, please refer to Video Settings on page 51.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

 Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

 Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen image.



 Start MP4 Recording: Click this button to record video clips in MP4 file format. Press the  Stop MP4 recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 22 for details.

 Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

Go to: Once the Administrator has determined the list of preset positions; you can aim the camera using this command. For more information, please refer to Camera Control on page 59.

Client Settings

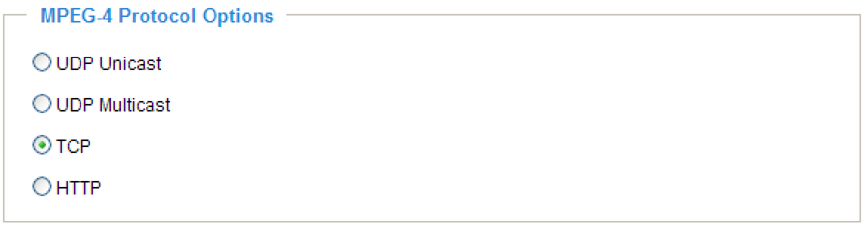
This chapter explains how to select the stream transmission mode and saving options on the local computer. When finished with the settings on this page, click **Save** on the bottom of the page to enable the settings.

MPEG-4 Media Options



Select whether to stream video or audio data or both. This is enabled only when the video mode is set to MPEG-4.

MPEG-4 Protocol Options



Depending on your network environment, there are four transmission modes for MPEG-4 streaming:

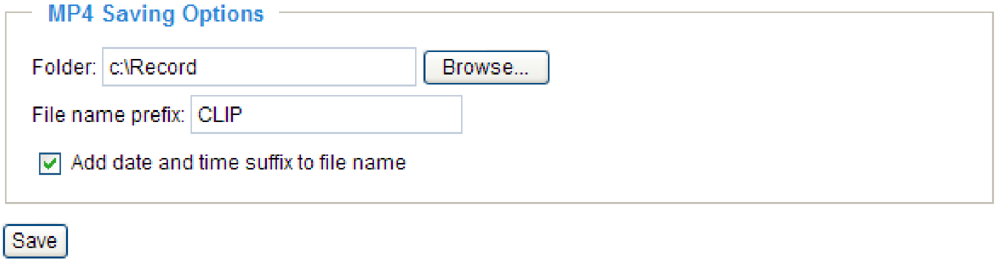
UDP unicast: This protocol allows for better real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate the UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 41.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. However, the real-time effect is not as good as that of the UDP protocol.

HTTP: This protocol allows for the same transmission quality as the TCP protocol without needing to open specific ports for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data through.

MP4 Saving Options

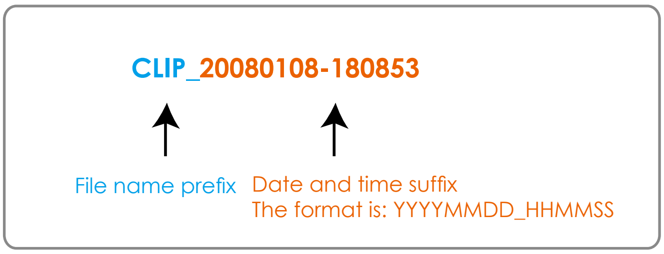


Users can record live video as they are watching by clicking Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

<u>Folder</u>: Specify the storage destination for the recorded video files.

<u>File name prefix</u>: Enter the text that will be appended to the front of the video file name.

<u>Add date and time suffix to the file name</u>: Select this option to append the date and time to the end of the file name.



Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only Administrators can access the configuration page.

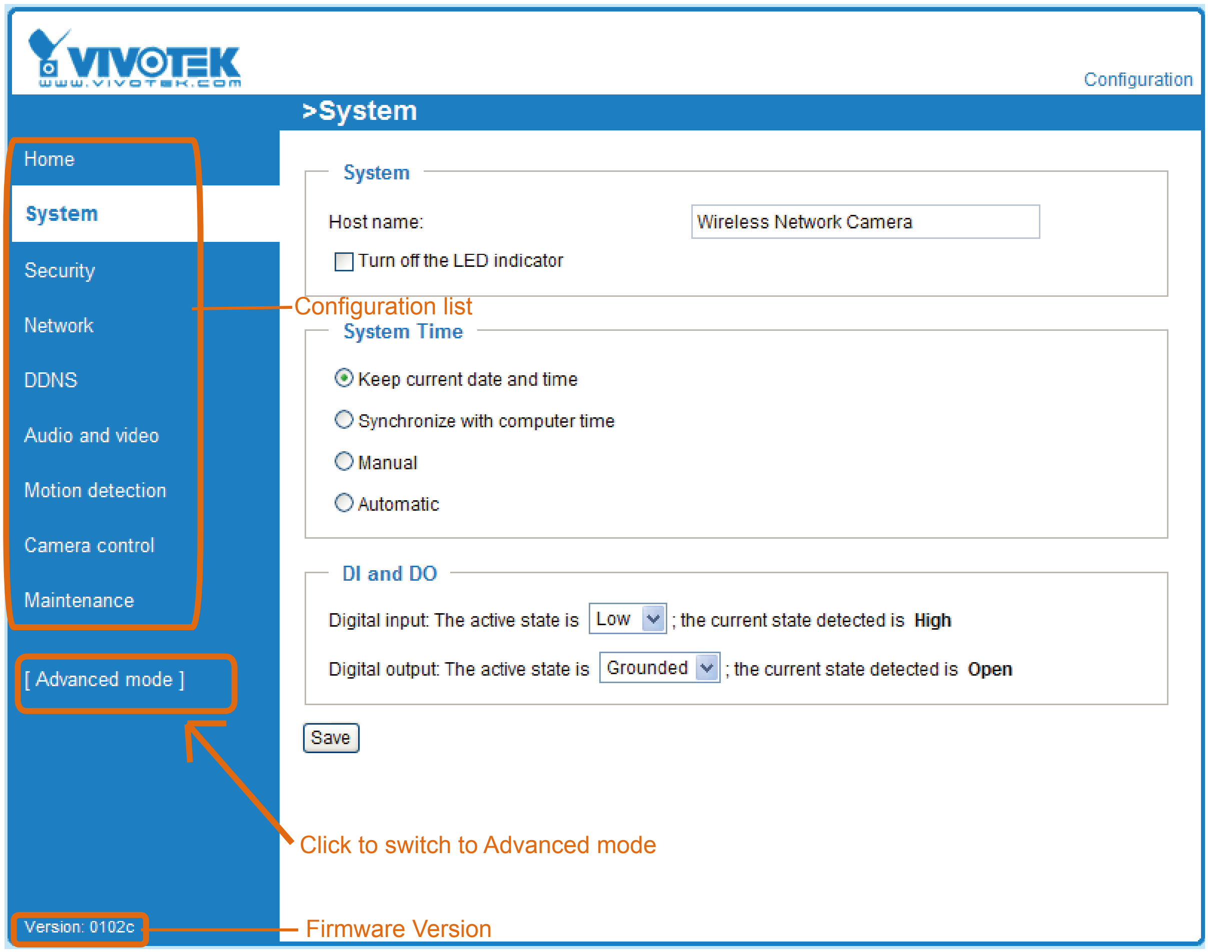
VIVOTEK offers an easy-to-use user interface that helps you set up your network camera with minimal effort. To simplify the setting procedure, two types of user interfaces are available: Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced functions (HTTPS/ Access list/ Homepage layout/ Application/ Recording/ System log/ View parameters) are not displayed in Basic Mode.

If you want to set up advanced functions, please click **[Advanced Mode]** on the bottom of the configuration list to quickly switch to Advanced Mode.

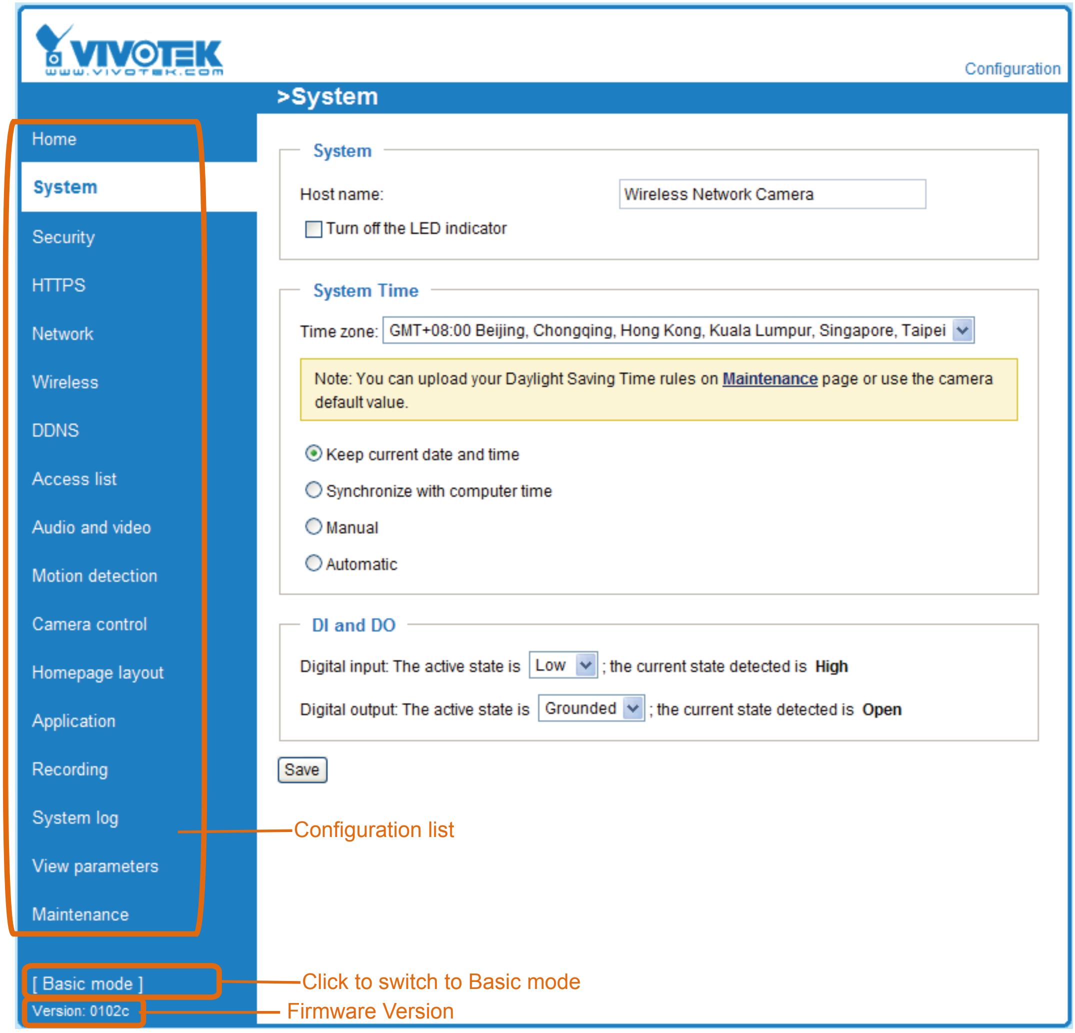
In order to simplify the user interface, the detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second sub-item will be displayed and that of the first sub-item will be hidden.

The following is the interface of the Basic Mode and the Advanced Mode:

Basic Mode



Advanced Mode

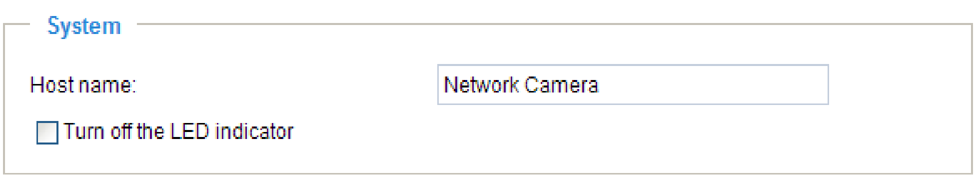


Each function on the configuration list will be explained in the following sections. Those functions that are displayed only in Advanced Mode are marked with Advanced Mode. If you want to set up the advanced functions, please click **[Advanced Mode]** on the bottom of the configuration list to quickly switch over.

System

This section explains how to configure the basic settings for the Network Camera, including System, System Time, and DI/DO. When completed with the settings on this page, click **Save** at the bottom of the page to enable the settings.

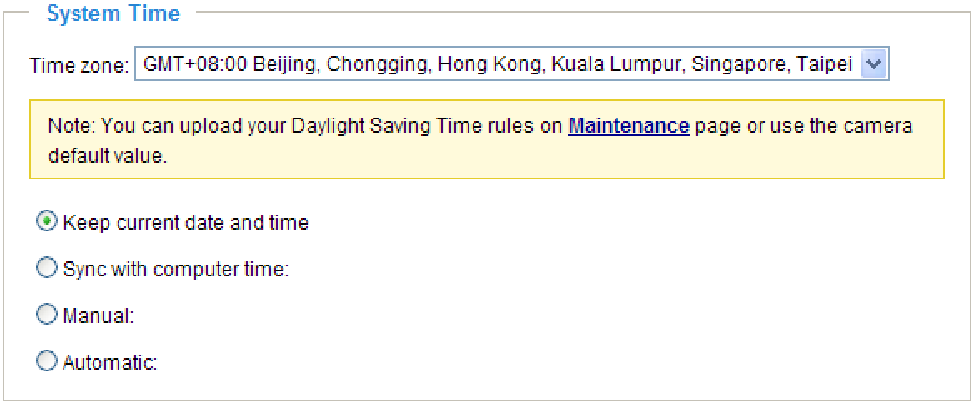
System



Host name: Enter the desired name for the Network Camera. The text will be displayed at the top of the main page.

Turn off the LED indicators: If you do not want to let others know that the network camera is in operation, you can select this option to turn off the LED indicators.

System Time



Keep current date and time: Select this option to preserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the system power is turned off.

Sync with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed when updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format is [yyyy/mm/dd] and [hh:mm:ss].

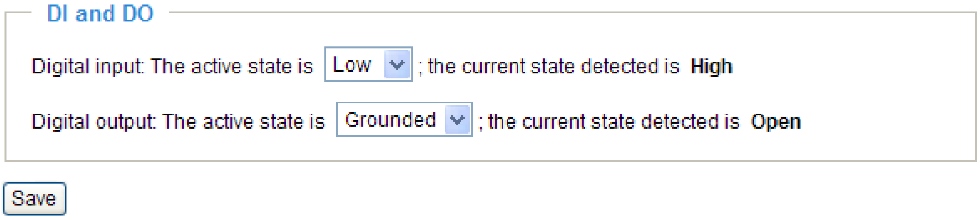
Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time servers.

Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Time zone Advanced Mode: Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules on the Maintenance page, please refer to Upload / Export Daylight Saving Time Configuration File on page 84 for details.

DI and DO



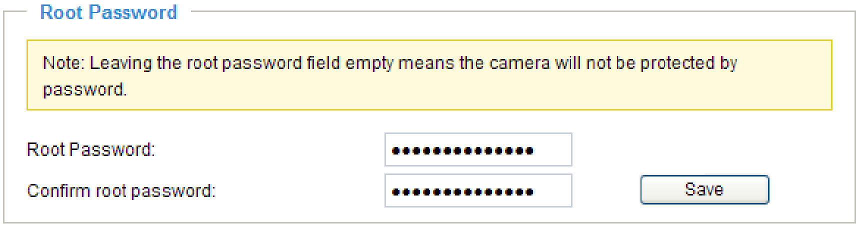
Digital input: Select **High** or **Low** to define the normal status for the digital input. The Network Camera will report the current status.

Digital output: Select **Grounded** or **Open** to define normal status for the digital output. The Network Camera will show whether the trigger is activated or not.

Security

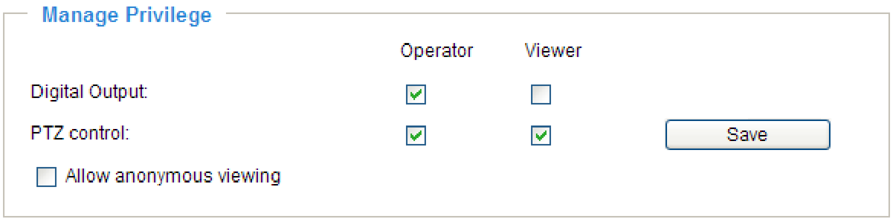
This section explains how to enable password protection and create multiple accounts.

Root Password



The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please set a password for the “root” account first.
1. Type the password in both text boxes, then click **Save** to enable password protection.
2. A window will be prompted for authentication; type the correct user’s name and password in their respective fields to access the Network Camera.

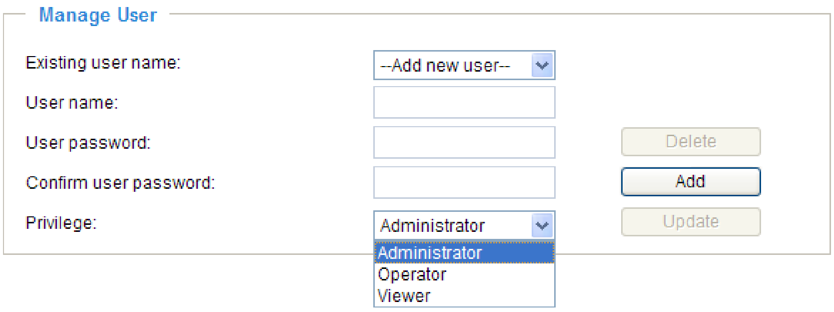
Manage Privilege Advanced Mode



Digital Output & PTZ control: You can modify the manage privilege of operators or viewers. Check or uncheck the item, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Main Page on page 17.)

Allow anonymous viewing: If you check this item, any client can access the live stream without entering a User ID and Password.

Manage User



Administrators can add up to 20 user accounts.
1. Input the new user’s name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Operators cannot access the Configuration page but can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands for the Network Camera on page 87. Viewers access only the main page for live viewing.

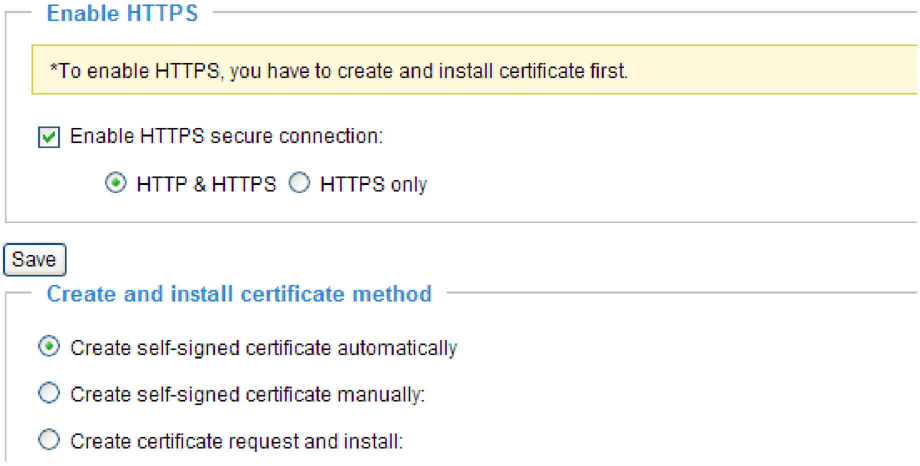
Here you also can change a user’s access rights or delete user accounts.
1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

HTTPS (Hypertext Transfer Protocol over SSL) Advanced Mode

This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Enable HTTPS

Check this item to enable HTTPS communication, then select a connection option: "HTTP & HTTPS" or "HTTPS only". Note that you have to create and install a certificate first in the second column before clicking the **Save** button.

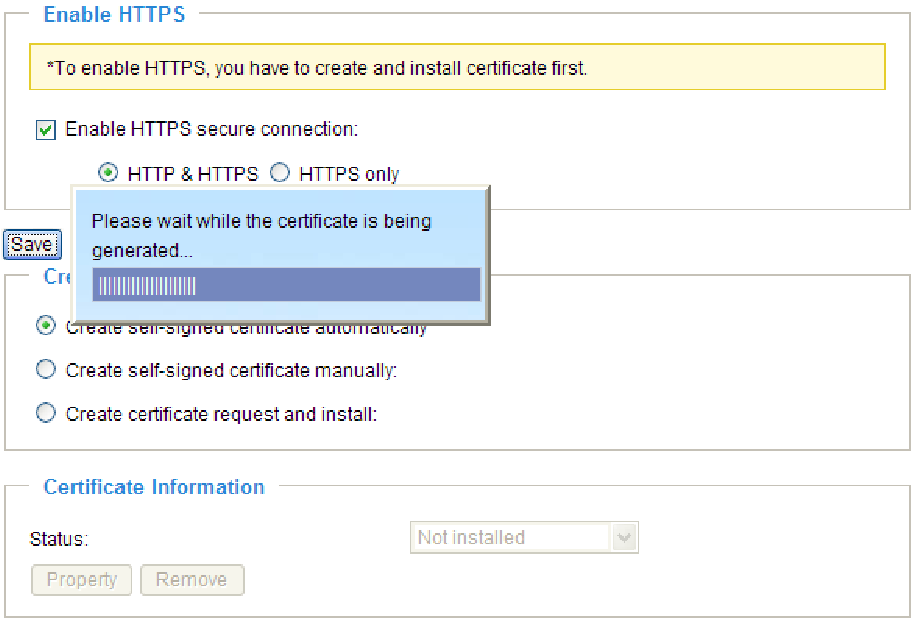


Create and Install Certificate Method

Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first. There are three ways to create and install a certificate:

Create self-signed certificate automatically

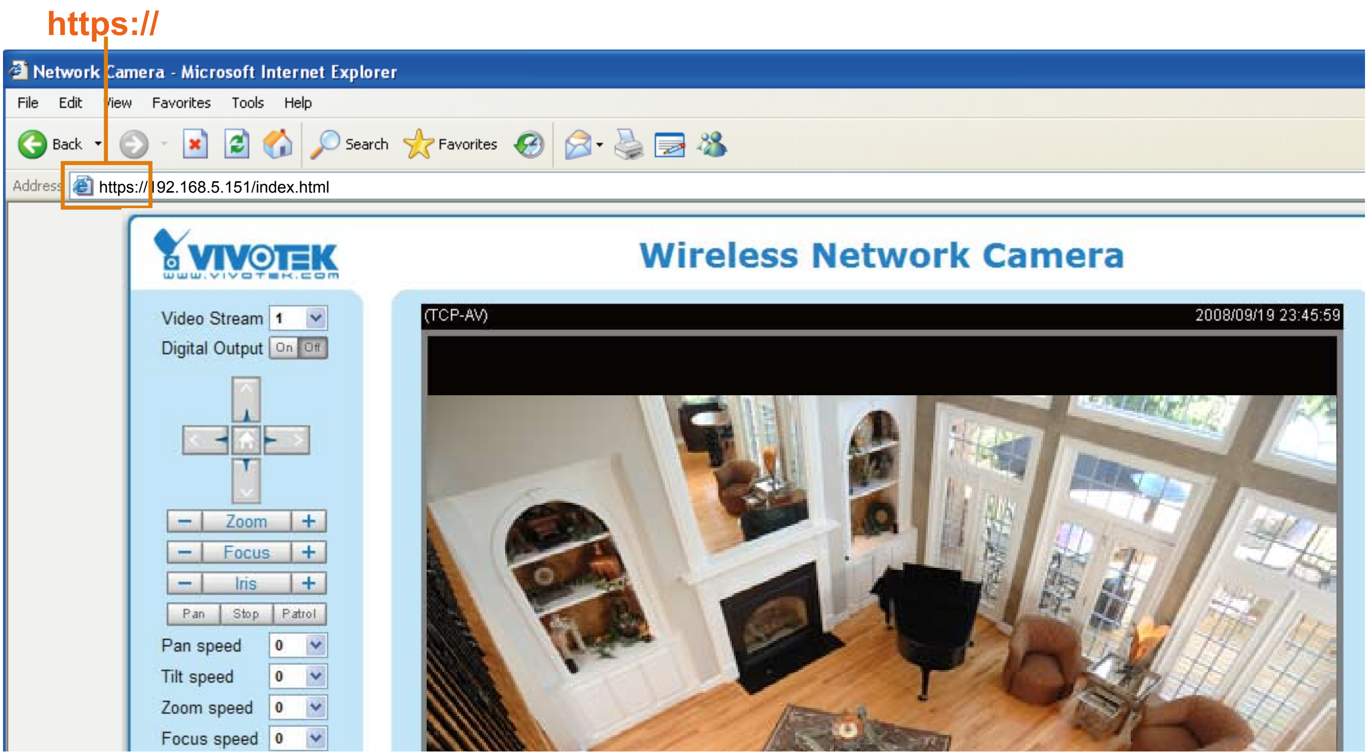
1. Select this option.
2. In the first column, check **Enable HTTPS secure connection**, then select a connection option: "HTTP & HTTPS" or "HTTPS only".
3. Click **Save** to generate a certificate.



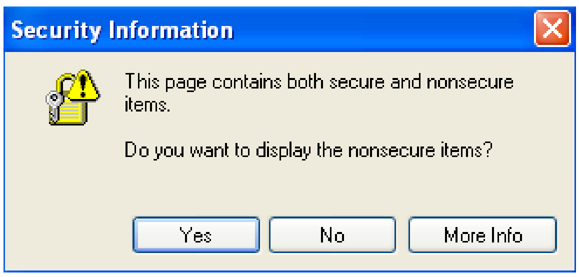
4. The Certificate Information will automatically de displayed in the third column as shown below. You can click **Property** to view detailed information about the certificate.



5. Click **Home** to return to the main page. Change the address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

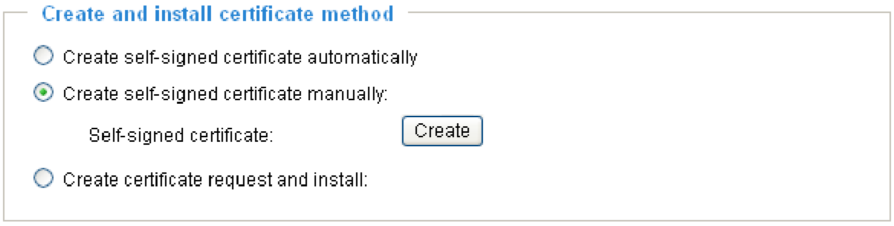


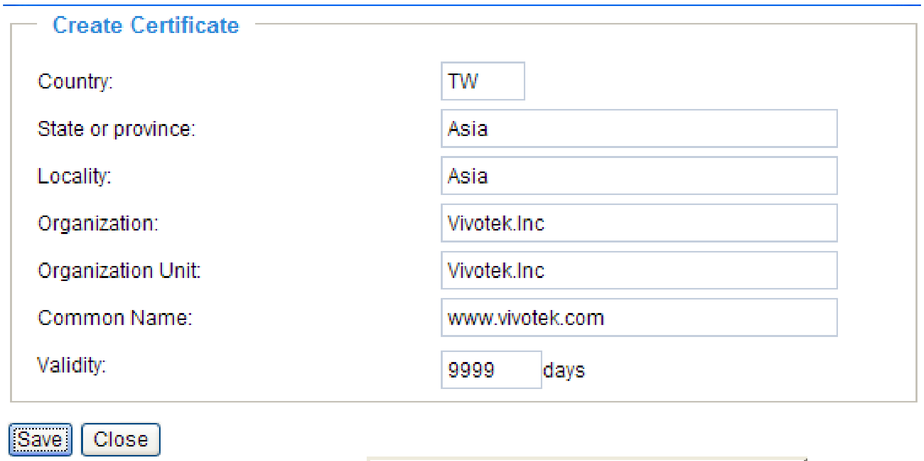


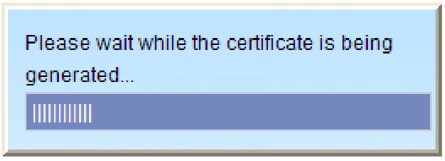


Create self-signed certificate manually

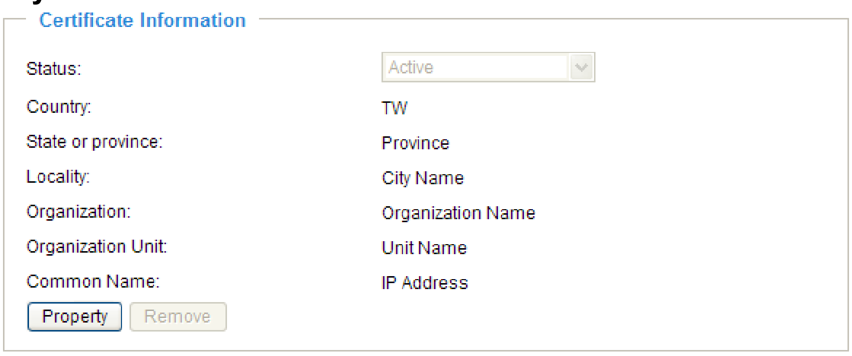
1. Select this option.
2. Click **Create** to open a Create Certificate page, then click **Save** to generate the certificate.





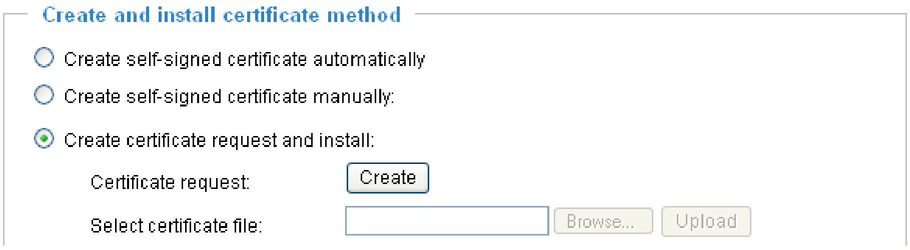


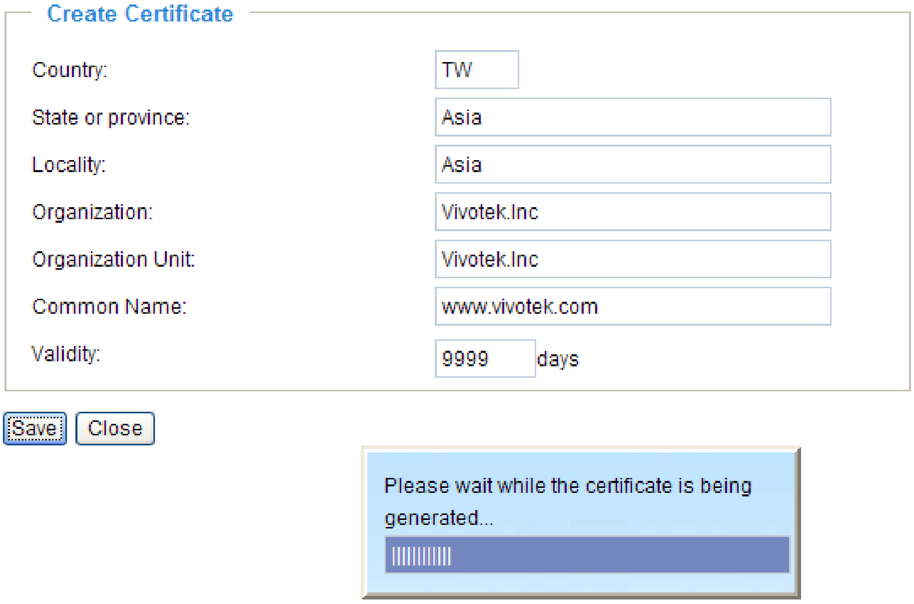
3. The Certificate Information will automatically be displayed in the third column as shown below. You can click **Property** to see detailed information about the certificate.



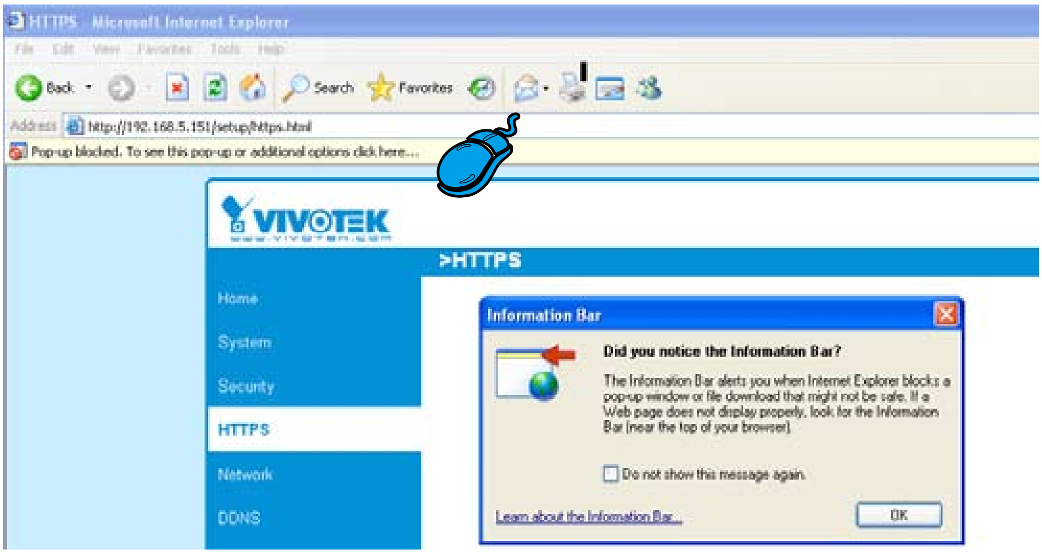
Create certificate and install : Select this option if you want to create an official certificate issued by a CA (Certificate Authority).

1. Select this option.
2. Click **Create** to open the Create Certificate page, then click **Save** to generate the certificate.

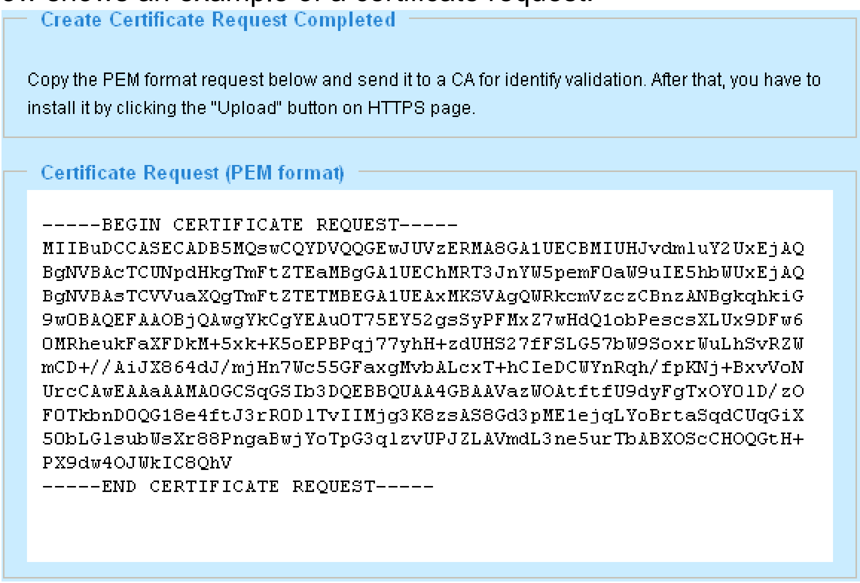




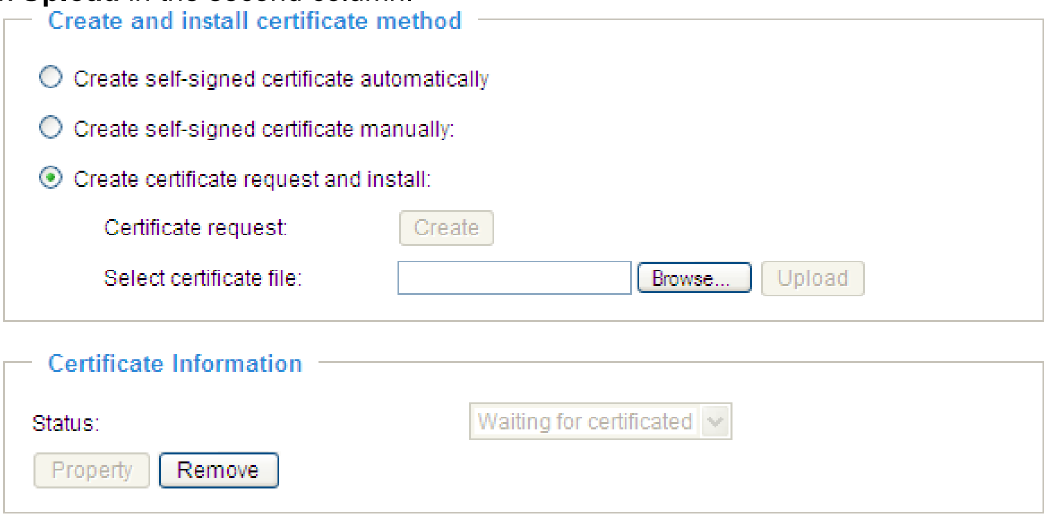
3. If you see the following Information bar, click **OK** and click on the Information bar on the top of the page to allow pop-ups.



4. The pop-up window shows an example of a certificate request.



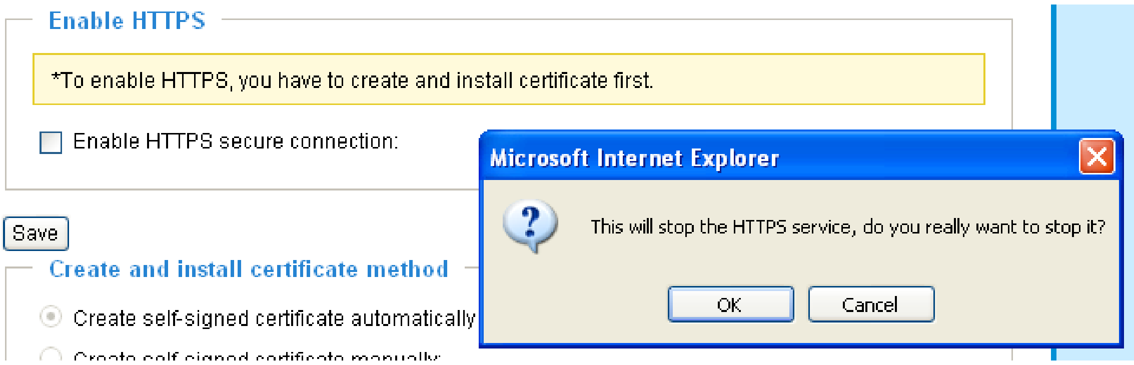
5. Look for a trusted certificate authority that issues digital certificates. Enroll the Network Camera. Wait for the certificate authority to issue a SSL certificate; click Browse... to search for the issued certificate, then click **Upload** in the second column.



NOTE

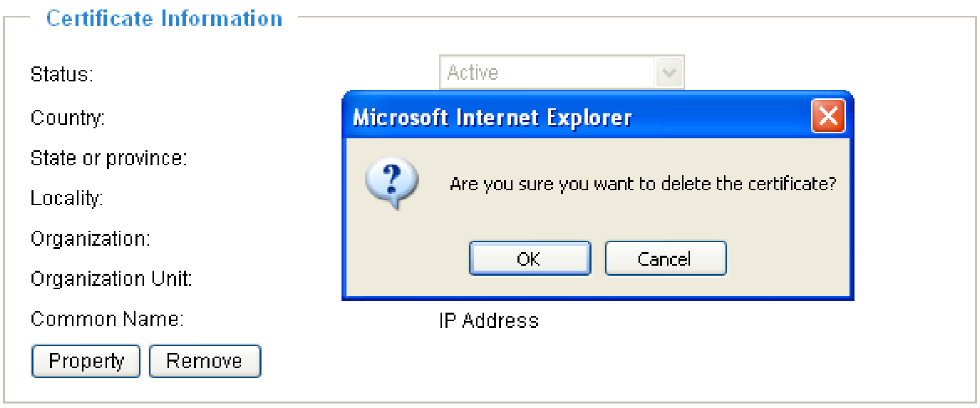
► *How do I cancel the HTTPS settings?*

1. *Uncheck **Enable HTTPS secure connection** in the first column and click **Save**; a warning dialog will pop up.*
2. *Click **OK** to disable HTTPS.*



3. *The webpage will redirect to a non-HTTPS page automatically.*

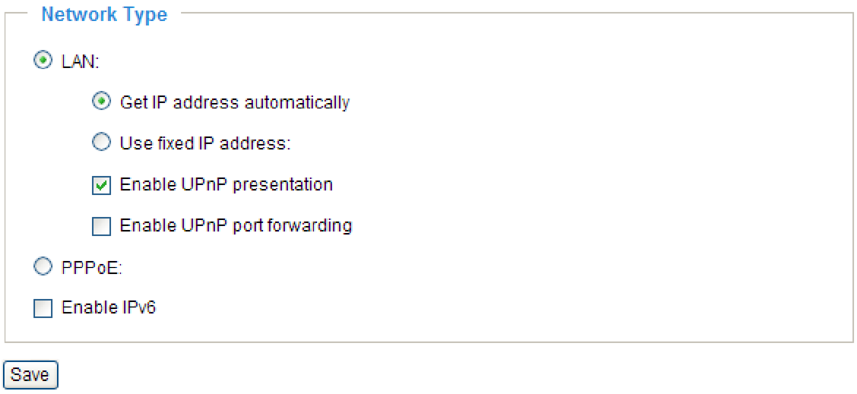
► *If you want to create and install other certificates, please remove the existing one. To remove the signed certificate, uncheck **Enable HTTPS secure connection** in the first column and click **Save**. Then click **Remove** to erase the certificate.*



Network

This section explains how to configure a wired network connection for the Network Camera.

Network Type

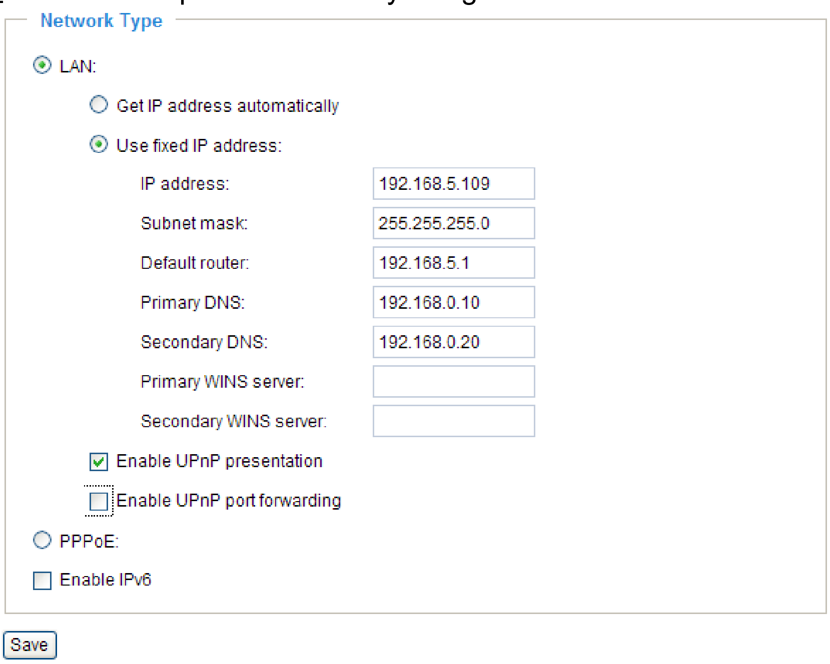


LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Rememer to click **Save** when you complete the Network setting.

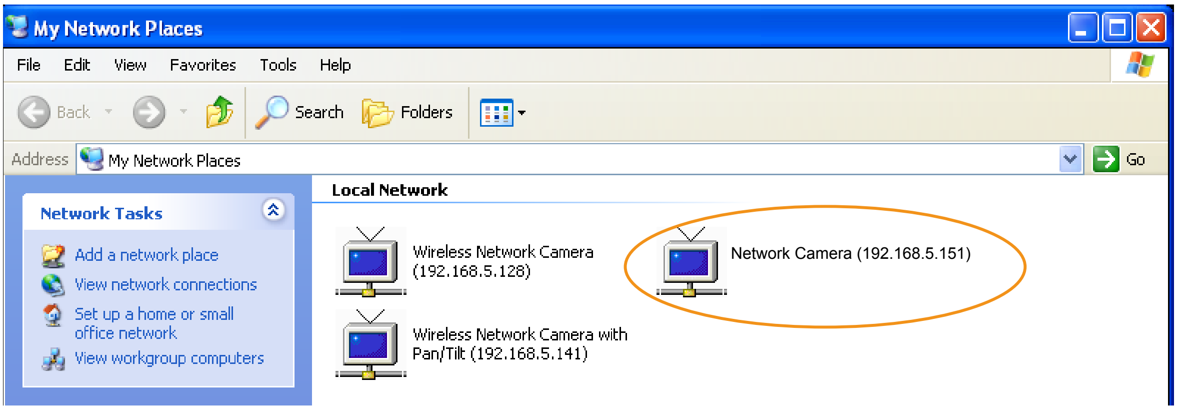
Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.



1. You can make use of VIVOTEK Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software Installation on page 11 for details.
2. Enter the static IP, Subnet mask, Default router, and Primary DNS provided by your ISP.

Enable UPnP presentation: Select this option to enable UPnP™ presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP™ component is installed on your computer.



Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP™ and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera on the LAN.
2. Go to Home > Configuration > Application > Server Settings (please refer to Server Settings on page 71) to add a new email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 74). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.



5. The Network Camera will reboot.
6. Disconnect the power to the Network Camera; remove it from the LAN environment.

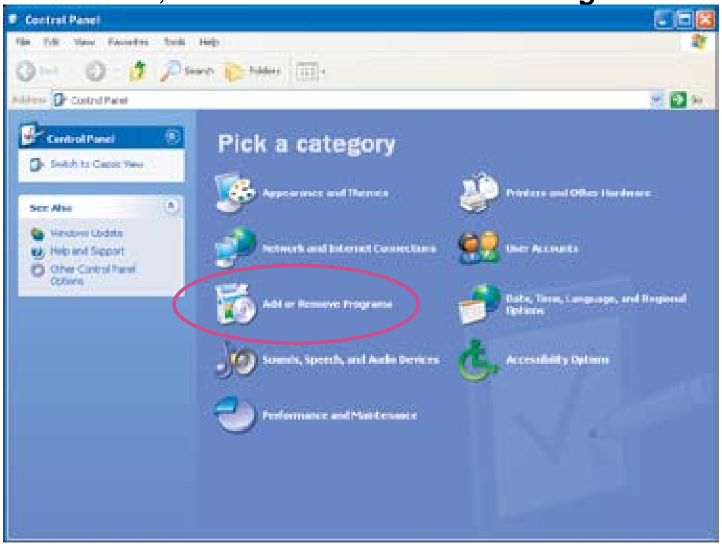
NOTE

► *If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.*

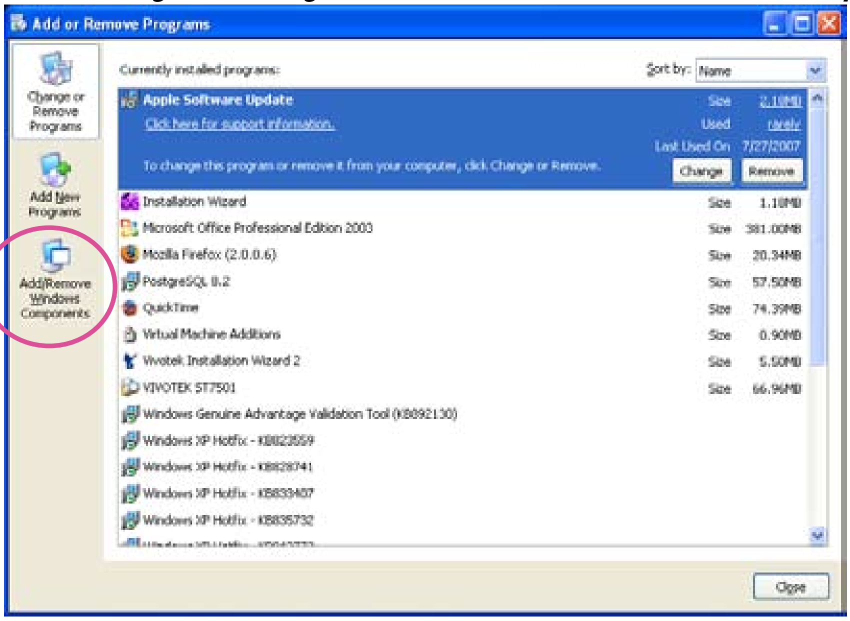
► *If UPnP™ is not supported by your router, you will see the following message:*
Error: Router does not support UPnP port forwarding.

► *Steps to enable the UPnP™ user interface on your computer:*
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

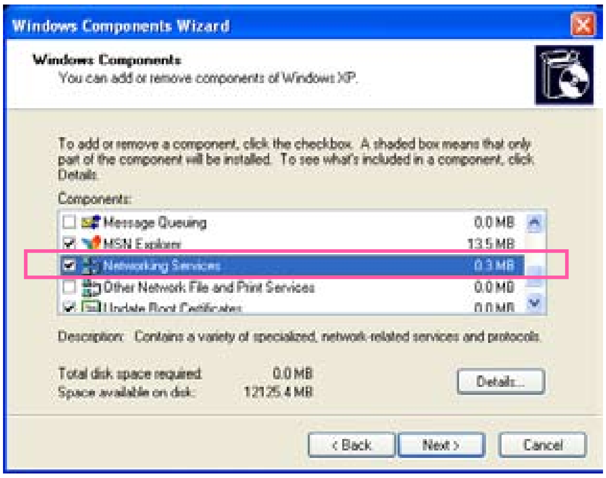
*1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.*



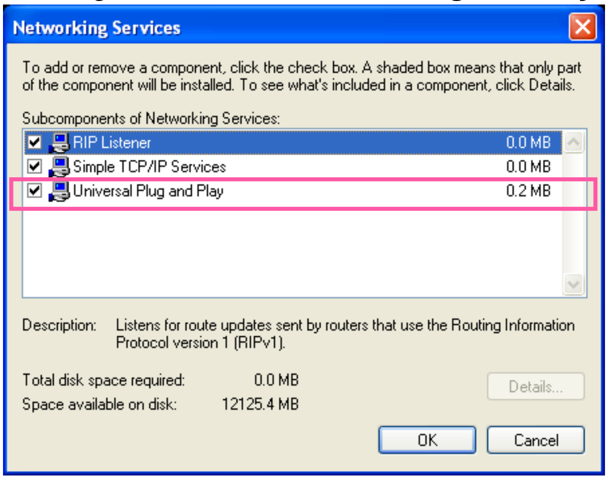
*2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.*



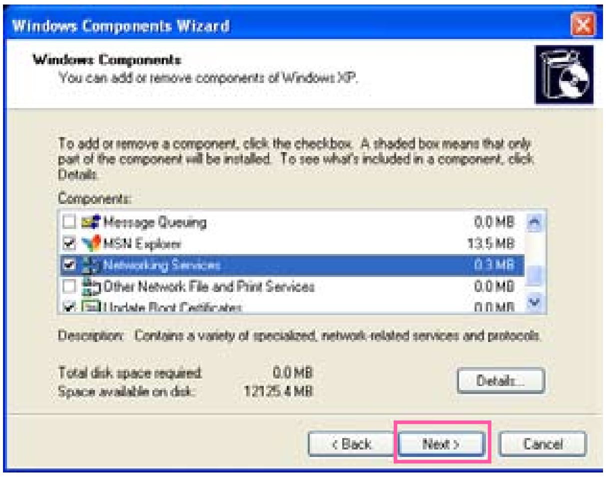
*3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.*



*4. In the Networking Services dialog box, select **Universal Plug and Play** and click **OK**.*



*5. Click **Next** in the following window.*



*6. Click **Finish**. UPnP™ is enabled.*

► *How does UPnP™ work?*
UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

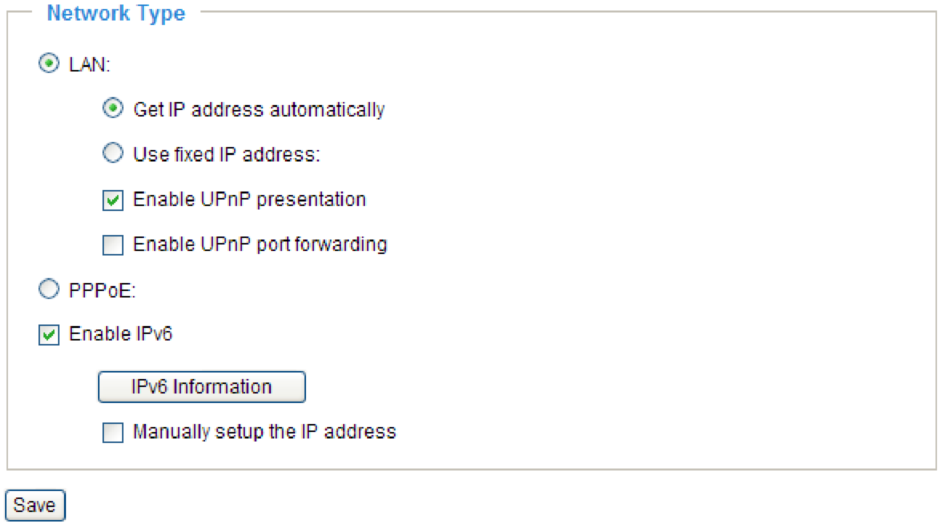
► *Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.*

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 83 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.*

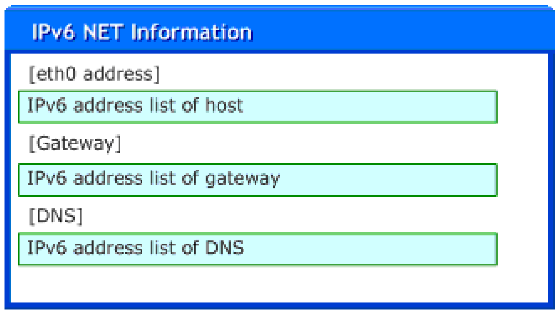
Enable IPv6

Select this option and click **Save** to enable IPv6 settings.
Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.

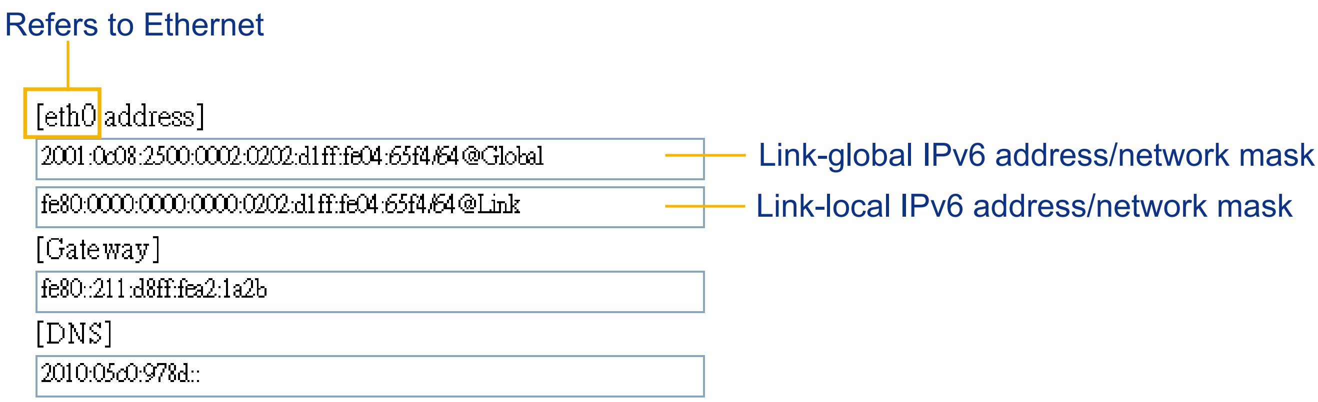


When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information as shown below.



If your IPv6 settings are successful, the IPv6 address list will listed in the pop-up window. The IPv6 address will be displayed as follows:

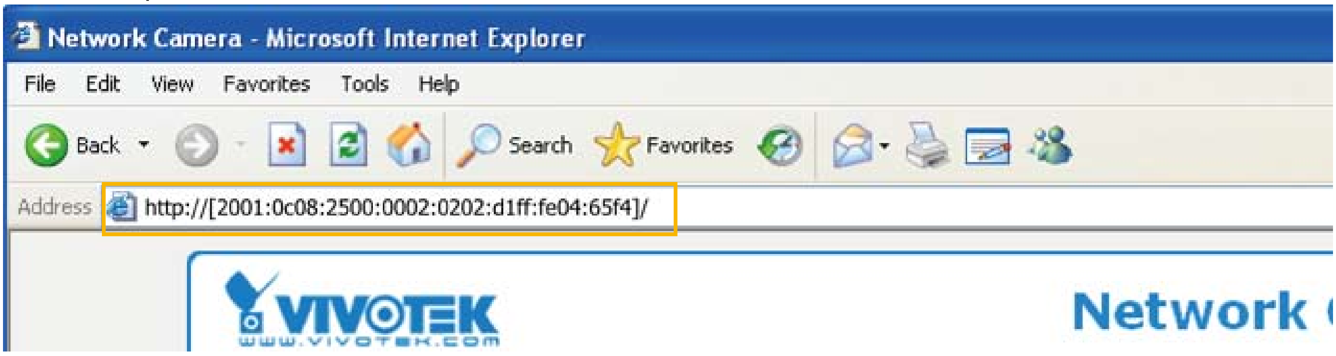


Please follow the steps below to link to an IPv6 address:
1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be:

http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/

↑ IPv6 address

4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
   For example:



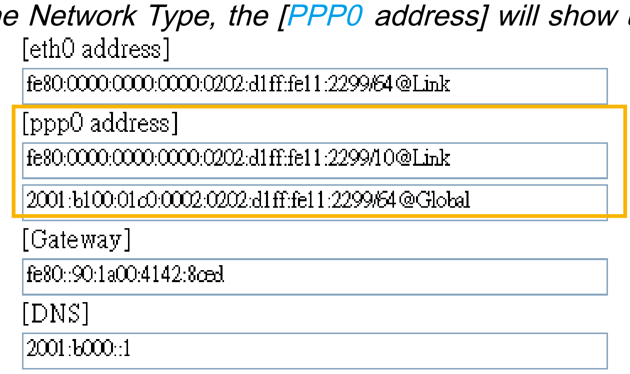
NOTE

► *If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to **HTTP** on page 38 for detailed information.)*

http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/:8080

↑ IPv6 address ↑ Secondary HTTP port

► *If you choose PPPoE as the Network Type, the [PPP0 address] will show up in the IPv6 information column as below.*

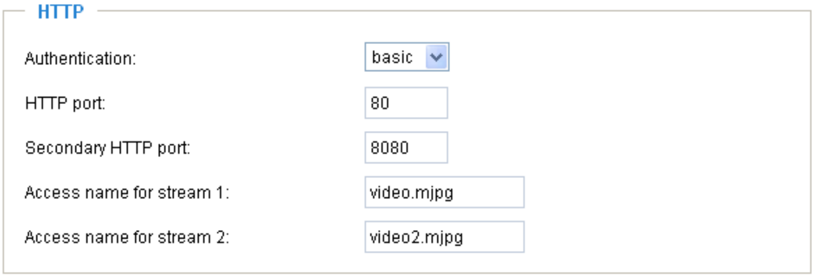


Manually setup the IP address: Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers.
If you check this item, the following blanks will be displayed for you to enter the corresponding information:



HTTP Advanced Mode

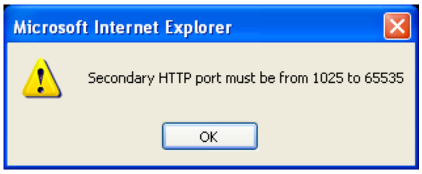
To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security on page 26 for details.



Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.
If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:





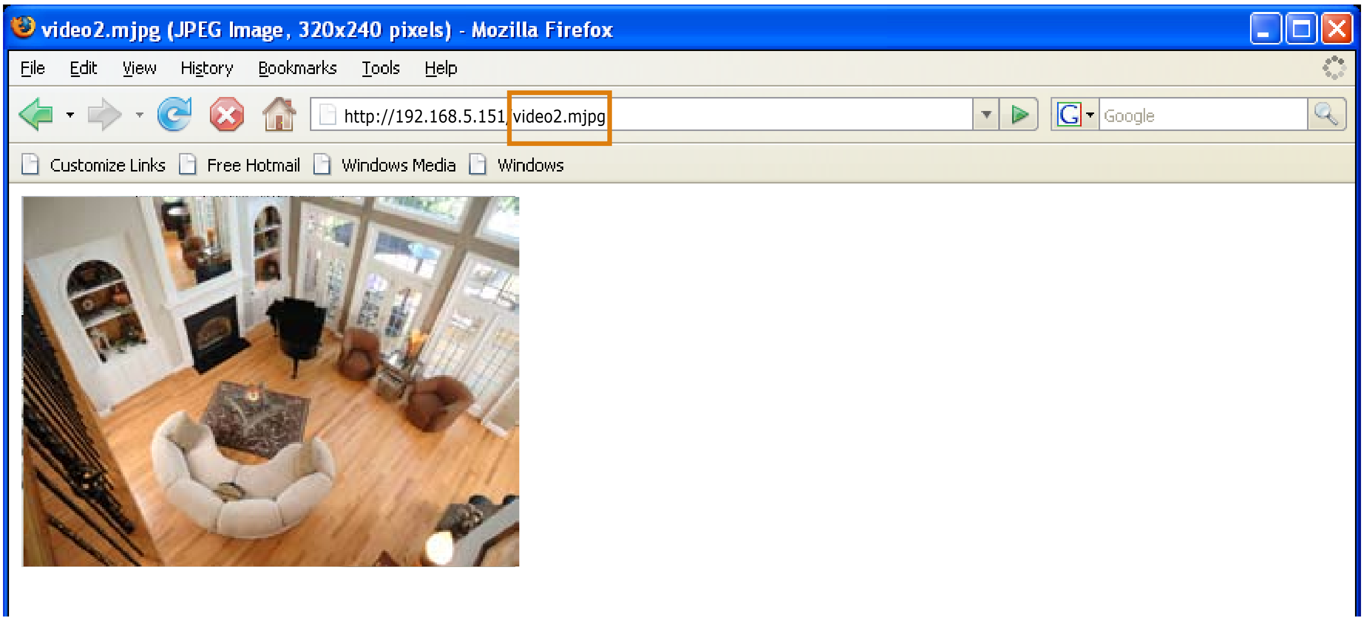
To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

In LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for stream 1 / Access name for stream 2: The access name is used to differentiate the streaming source.

When using Mozilla Firefox or Netscape to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.

URL command -- http://<ip address>:<http port>/<access name for stream1 or stream2>
For example, when the Access name for stream 2 is set to video2.mjpg:
1. Launch Mozilla Firefox or Netscape.
2. Type the URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.



NOTE

► *Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream1 or stream2> will fail to access the Network Camera.*

HTTPS



By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

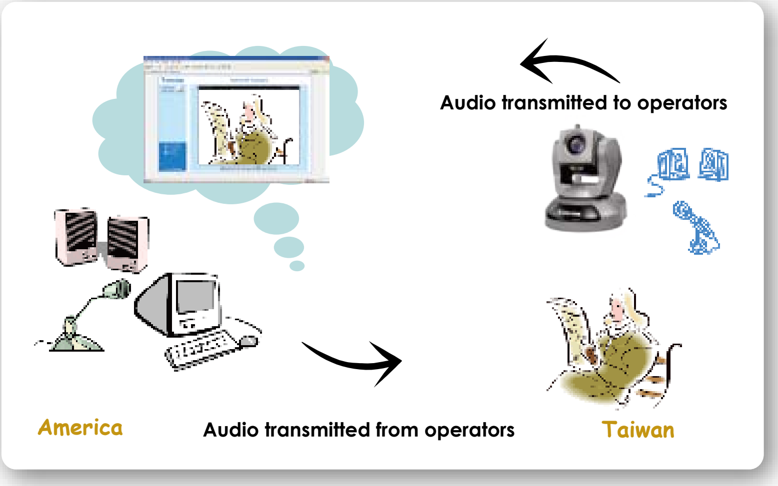
Two way audio

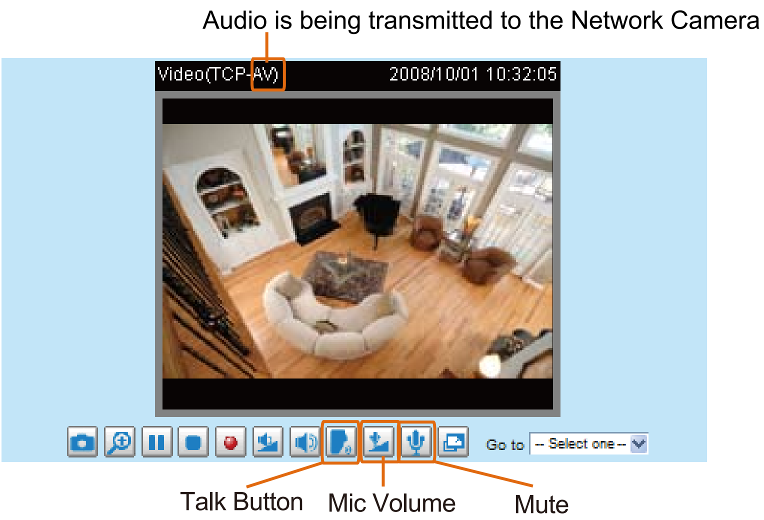


By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in or external microphone and an external speaker, you can communicate with people around the Network Camera.

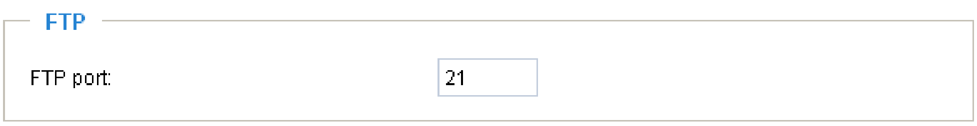
Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to “MPEG-4” on the Audio and Video Settings page and the media option is set to “Video and Audio” on the Client Settings page. Please refer to Client Settings on page 21 and Audio and Video Settings on page 51.





Click [Talk] to enable audio transmission to the Network Camera; click [Mic Volume] to adjust the volume of microphone; click [Mute] to turn off the audio. To stop talking, click [Talk] again.

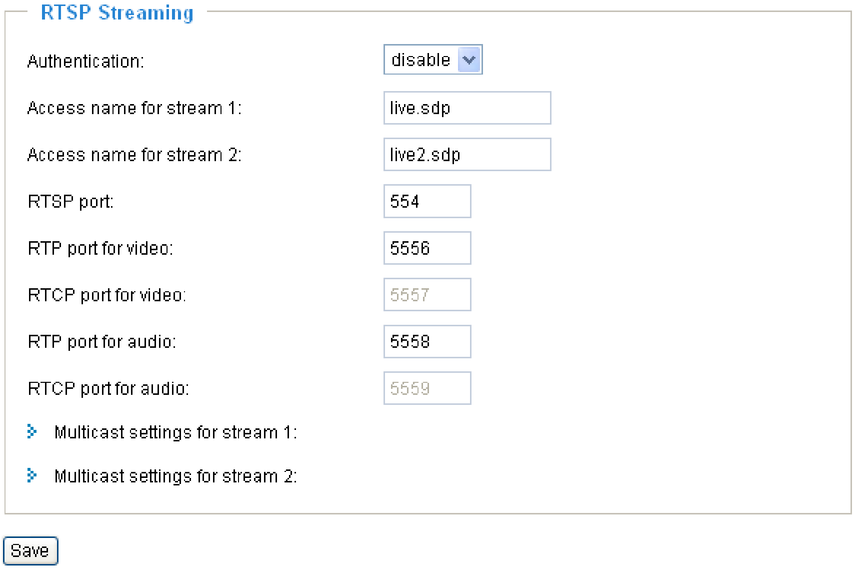
FTP



The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK Installation Wizard 2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to another port number between 1025 and 65535.

RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the Network Camera first; please refer to Security on page 26 for details.



Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.
If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.

The availability of the RTSP streaming for the three authentication modes is listed in the following table:

	Quick Time player	Real Player
Disable	O	O
Basic	O	O
Digest	O	X

Access name for stream 1 / Access name for stream 2: This Network camera supports dual streams simultaneously. The access name is used to differentiate the streaming source.
If you want to use an RTSP player to access the Network Camera, you have to set the video mode to MPEG-4 and use the following RTSP URL command to request transmission of the streaming data.

rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>
For example, when the access name for stream 1 is set to live.sdp:

1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the URL command in the text box. For example:
4. The live video will be displayed in your player as shown below.





RTSP port /RTP port for video, audio/ RTCP port for video, audio

- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

- The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

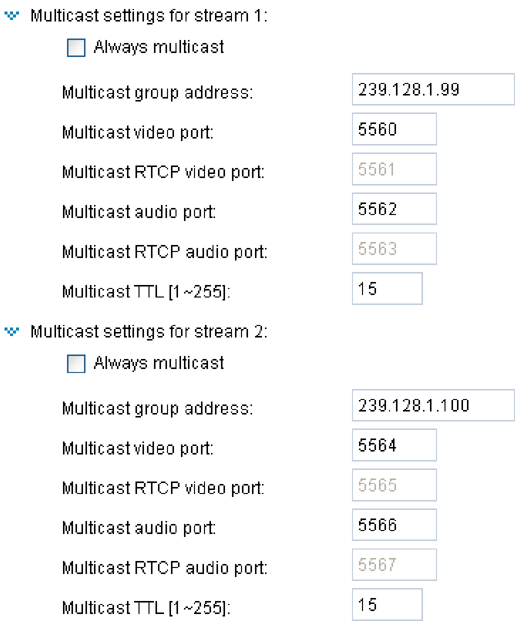
- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always odd. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:



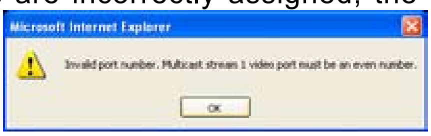
Multicast settings for stream 1 / Multicast settings for stream 2: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 or stream 2.



Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

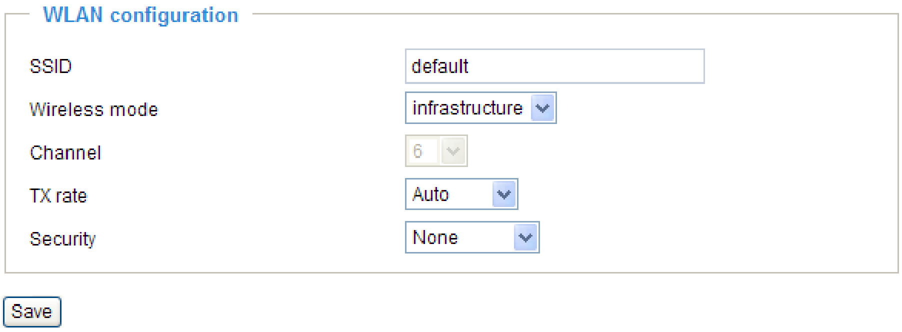
The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and is thus always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:



Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

Wireless LAN (PZ7112/PZ7122 only)

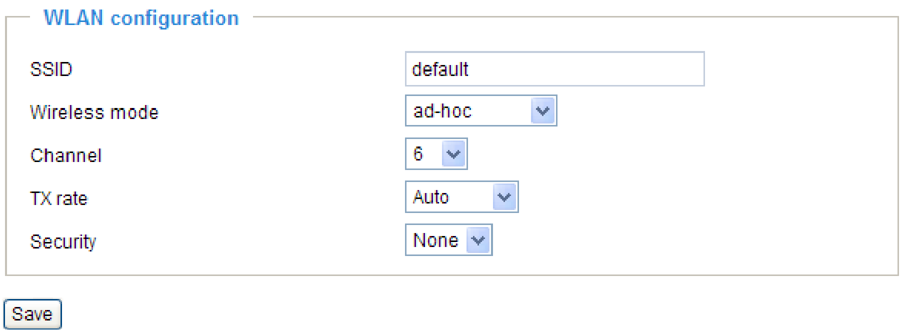


SSID (Service Set Identifier): This is the name that identifies a wireless network. Access Points and wireless clients attempting to connect to a specific WLAN (Wireless Local Area Network) must use the same SSID. The default setting is “default”. Note: The maximum length for an SSID is 32 single-byte characters and cannot consist of “, <, >, or blank spaces.

Wireless mode: Click on the pull-down menu to select from the following options:

■ Infrastructure: Connect the Network Camera to the WLAN via an Access Point. (default setting)

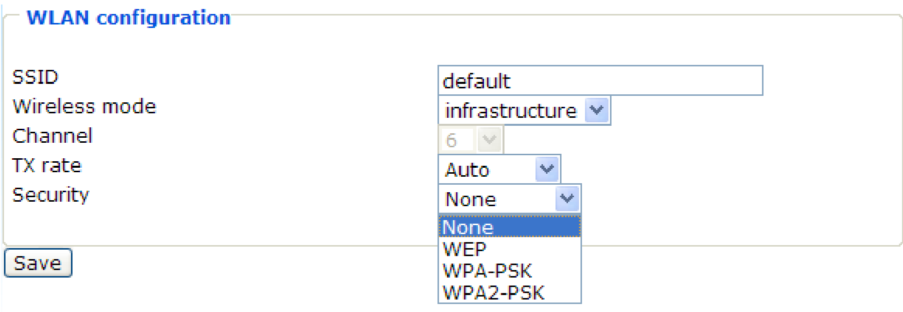
■ Ad-Hoc: Connect the Network Camera directly to a host equipped with a wireless adapter in a peer-to-peer environment.



Channel: While in infrastructure mode, the channel is selected automatically to match the channel setting of the selected Access Point. In Ad-Hoc mode, the channel must be manually set to the same channel for each wireless adapter. The default channel setting depends on the installed region.

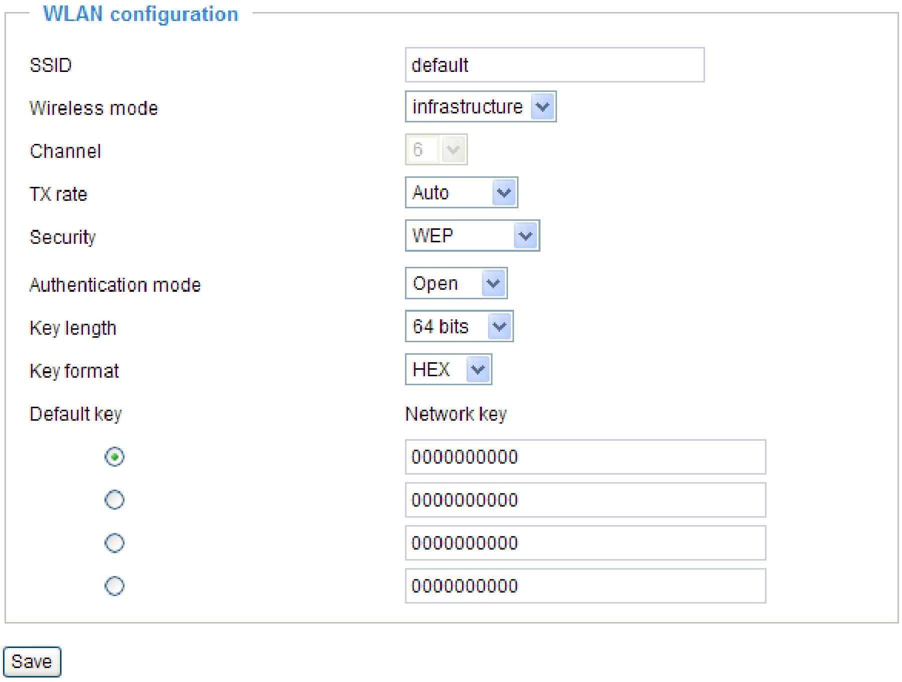
TX rate: This field is for selecting the maximum transmission rate over the network. The default setting is “auto”, that is, the Network Camera will try to connect to other wireless devices with highest transmission rate.

Security: Select the data encrypt method. There are four types, including: none, WEP, WPA-PSK, and WPA2-PSK.



1. None: No data encryption.

2. WEP (Wired Equivalent Privacy): This allows communication only with other devices with identical WEP settings.



■ Authentication Mode: Choose one of the following modes. The default setting is “Open”.
<u>Open</u> – Communicates the key across the network.
<u>Shared</u> – Allows communication only with other devices with identical WEP settings.

■ Key length: The administrator can set the key length to 64 or 128 bits.
The default setting is “64 bits”.

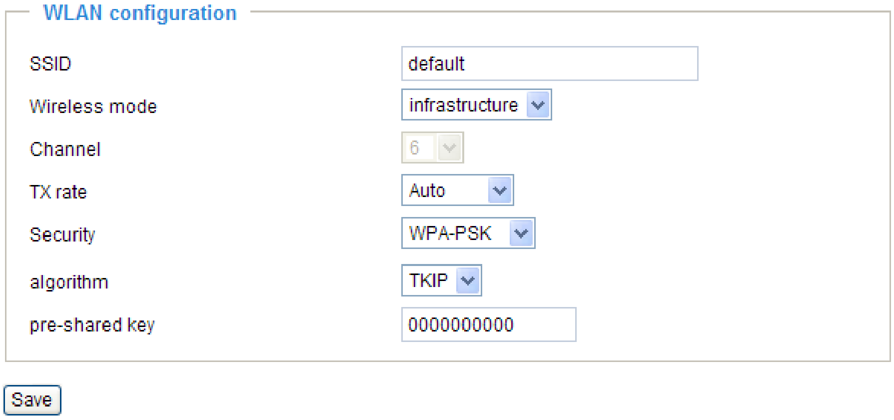
■ Key format: Hexadecimal or ASCII. The fault setting is “HEX”.
<u>HEX</u> digits consist of the numbers 0~9 and the letters A-F.
<u>ASCII</u> is a code for representing English letters as numbers from 0-127 except “, <, > , and the space character which are reserved.

■ Network Key: Enter a key in either hexadecimal or ASCII format.
You can select different key lengths, the acceptable input lengths are as follows:
64-bit key length: 10 Hex digits or 5 characters.
128-bit key length: 26 Hex digits or 13 characters.

<u>NOTE</u>

► *When 22(“), 3C(<), or 3E(>) are input as network keys, the key format cannot be changed to ASCII format.*

3. WPA-PSK: Use WPA (Wi-Fi Protected Access) pre-shared key.



More secure than WEP, the Wi-Fi Alliance developed WPA (Wi-Fi Protected Access) in 2003 to address WEP's weaknesses. Improvements included TKIP, which changes the encryption key for each data transmission.

■ Algorithm: Choose one of the following algorithms for WPA-PSK and WPA2-PSK modes.
TKIP (Temporal Key Integrity Protocol): A security protocol used in IEEE 802.11 wireless networks. TKIP is a "wrapper" that goes around the existing WEP encryption. TKIP is comprised of the same encryption engine and RC4 algorithm defined for WEP; however, the key used for encryption in TKIP is 128 bits long. This solves the first problem of WEP: a short key length. (From Wikipedia)

AES (Advanced Encryption Standard): In cryptography, the Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography. (From Wikipedia)

■ Pre-shared Key: Enter a key in ASCII format. The length of the key can be between 8 to 63 characters.

4. WPA2-PSK: Use WPA2 pre-shared key.
This advanced protocol, certified through Wi-Fi Alliance's WPA2 program, implements the mandatory elements of 802.11i. In particular, it introduces a new AES-based algorithm, CCMP, that is considered fully secure. From March 13, 2006, WPA2 certification is mandatory for all new devices wishing to be certified by the Wi-Fi Alliance as "Wi-Fi CERTIFIED." (From Wikipedia)

NOTE

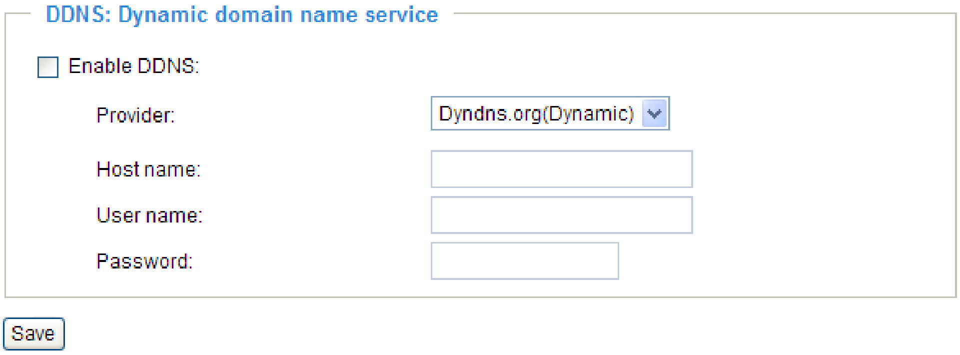
► *After wireless configurations are completed, click **Save** and the camera will reboot. Wait for the live image ito be reloaded to your browser. For VIVOTEK 7000-series cameras, you have to unplug the power and Ethernet cables from the camera; then re-plug the power cable to the camera. The camera will switch to wireless mode.*

► *Some invalid settings may cause the system to fail to respond. Change the configuration settings only if necessary and consult with your network supervisor or experienced users for correct settings. Once the system has lost contact, please refer to Maintenance on page 83 for reset and restore procedures.*

DDNS

This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

DDNS: Dynamic domain name service

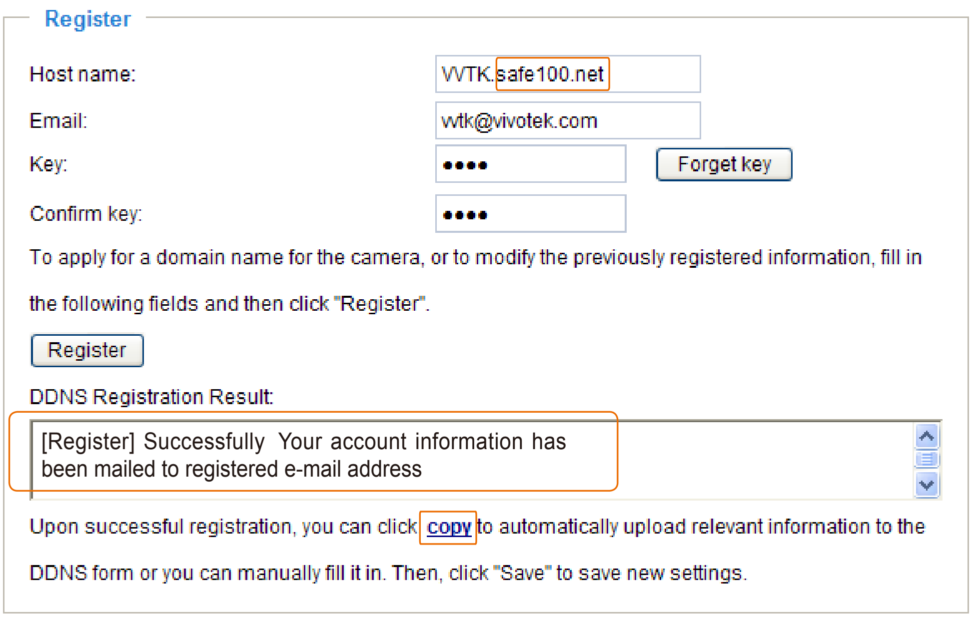


Enable DDNS: Select this option to enable the DDNS setting.

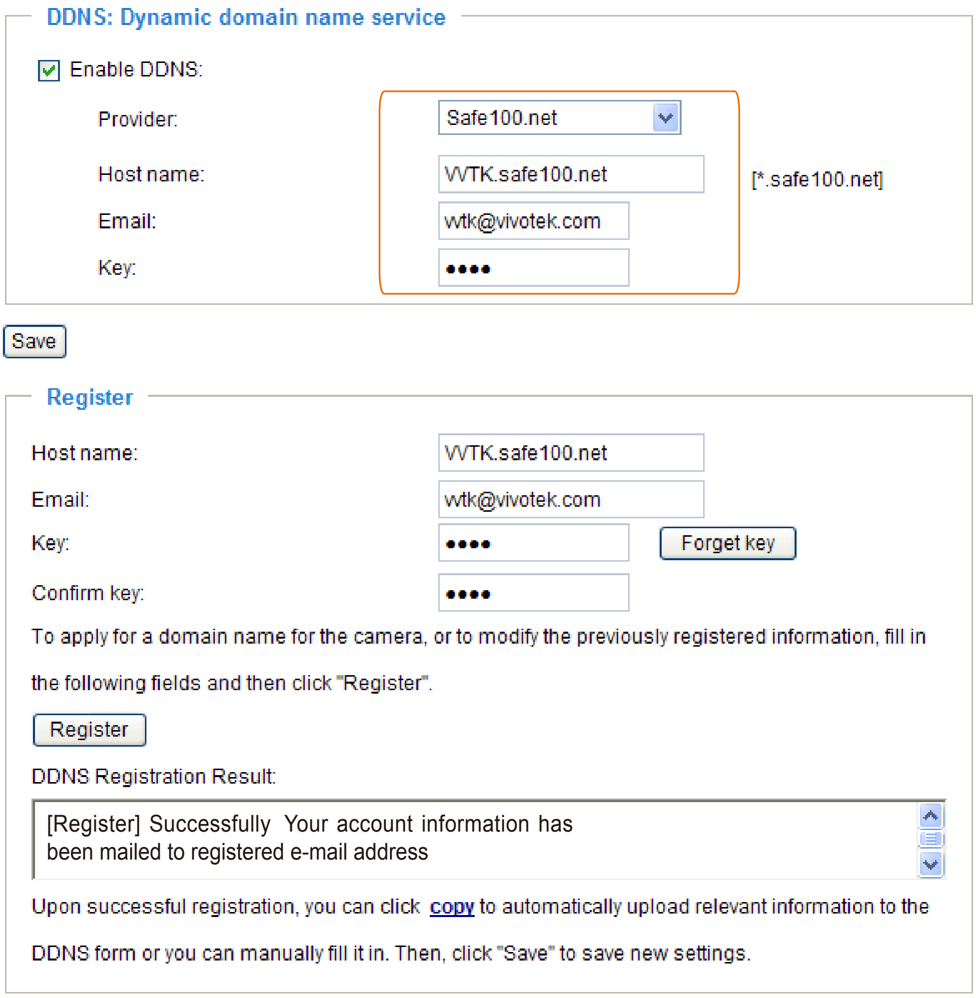
Provider: Select a DDNS provider from the provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.
Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, then click **Register**. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.



3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the picture.



4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

VIVOTEK offers documents to establish a CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Email, Key, and Confirm Key; then click **Register**. After a host name has been successfully created, you will see a success message in the DDNS Registration Result column.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.

Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your account information will be sent to your email address.

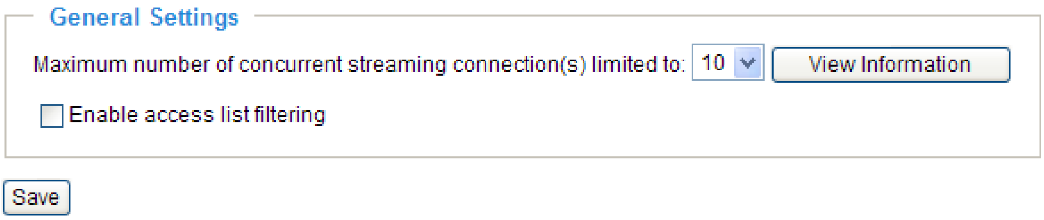
Refer to the following links to apply a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/
■ TZO.com: visit http://www.tzo.com/
■ DHS.org: visit http://www.dhs.org/
■ dyn-interfree.it: visit http://dyn-interfree.it/

Access List Advanced Mode

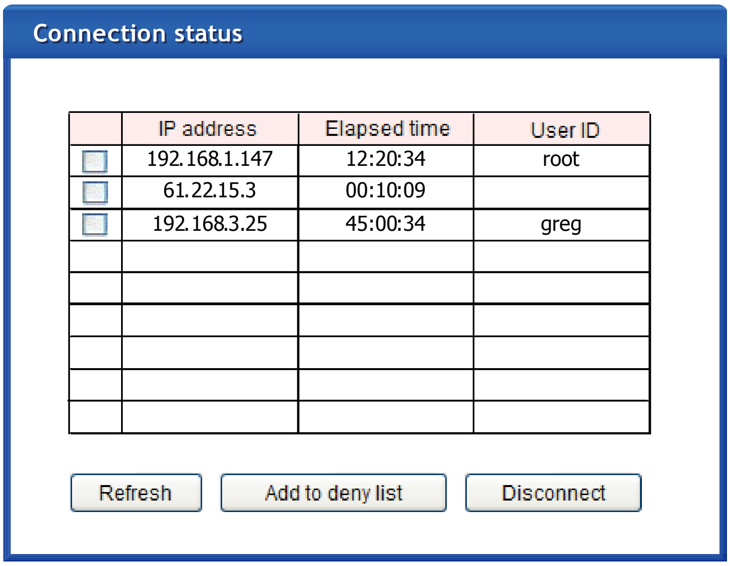
This section explains how to control access permission by verifying the client PC's IP address.

General Settings



Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 and stream 2). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explore or Quick Time Player).

View Information: Click this button to display the connection status window showing a list of the current connections. For example:



■ IP address: Current connections to the Network Camera.

■ Elapsed time: How much time the client has been at the webpage.

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column will be empty.

There are some situations which allow clients access to the live video without a user name and password:

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security on page 26.
2. The administrator has set up a root password, but set **RTSP Authentication** to "disable". For more information about **RTSP Authentication**, please refer to RTSP Streaming on page 41.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing**, please refer to Security on page 26.

■ Refresh: Click this button to refresh all current connections.

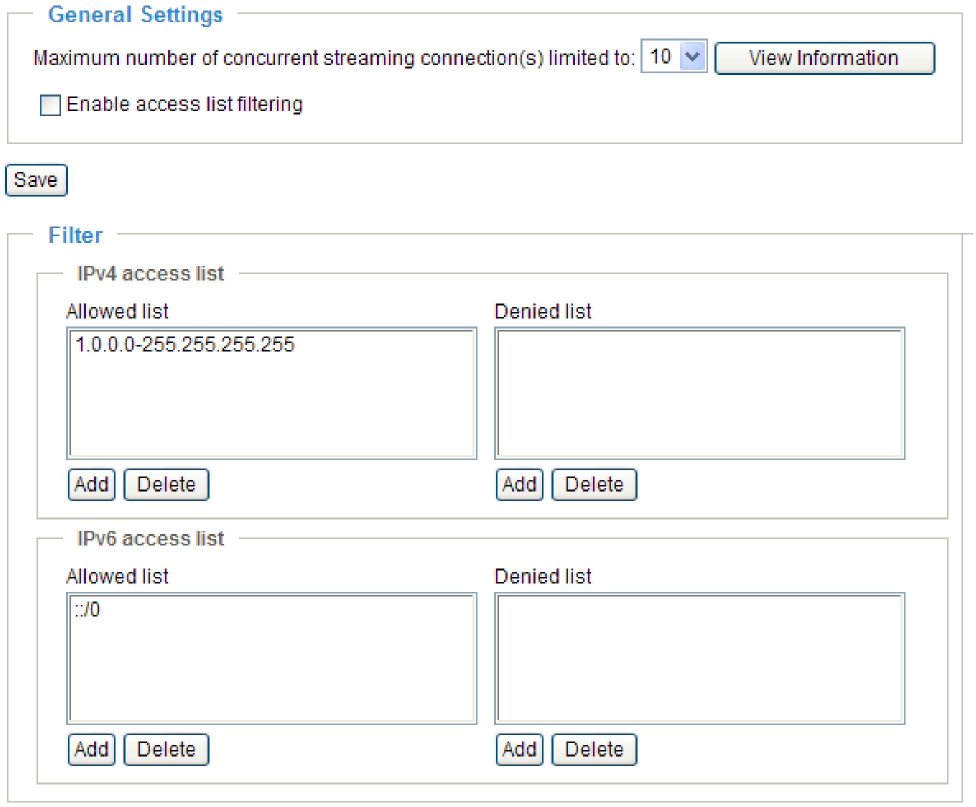
■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the denied list, please check **Enable access list filtering** and click **Save** in the first column.

■ Disconnect: If you want to break off the current connections, please select them and click this button. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player).

Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

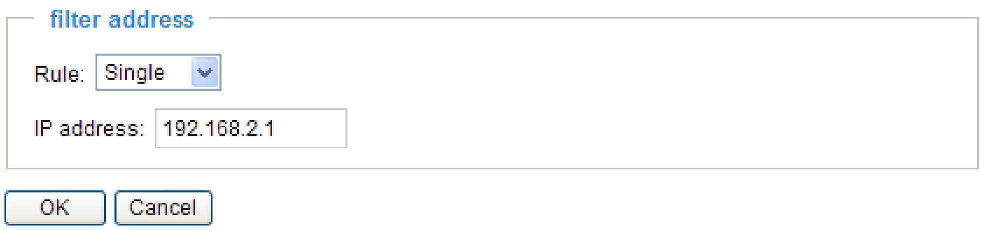
Filter

There are two lists for permission control: Allowed list and Denied list. Only those clients whose IP addresses are on the Allowed list and not on the Denied list can access the Network Camera. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to page 36 for detailed information.

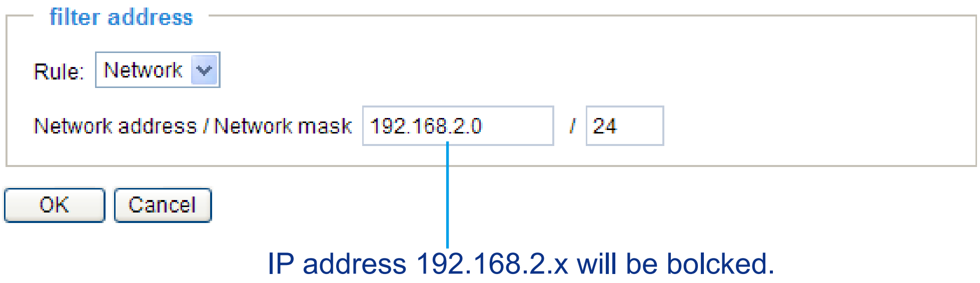


■ Add a rule to Allowed/Denied list: Click **Add** to add a rule to Allowed/Denied list.

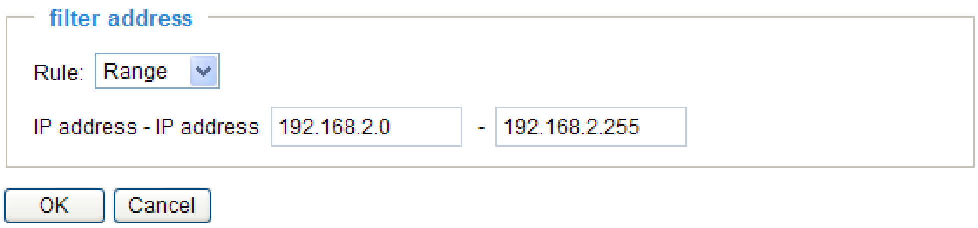
There are three types of rules for user to set up:
Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:



Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List.
For example:



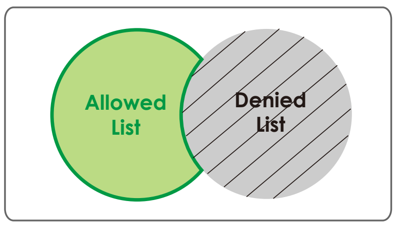
Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List. This rule is only applied to IPv4.
For example:



■ Delete Allowed/Denied list:
In the Delete Allowed List or Delete Denied List column, make a selection and click **Delete**.

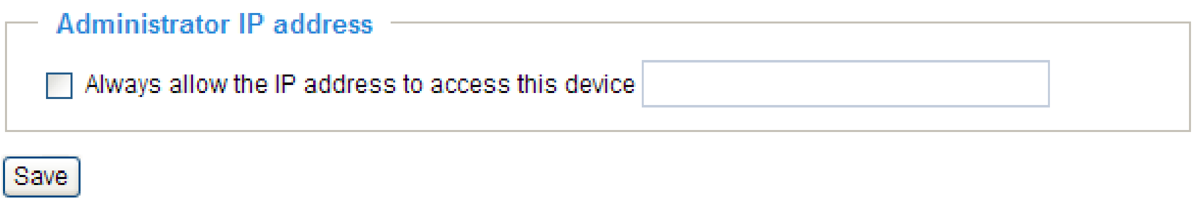
NOTE

► *For example, when the range of IP addresses in the allowed list is set from 1.1.1.0 to 192.255.255.255 and the range in the denied list is set from 1.1.1.0 to 170.255.255.255, only users' IP located between 171.0.0.0 and 192.255.255.255 can access the Network Camera.*



Administrator IP address

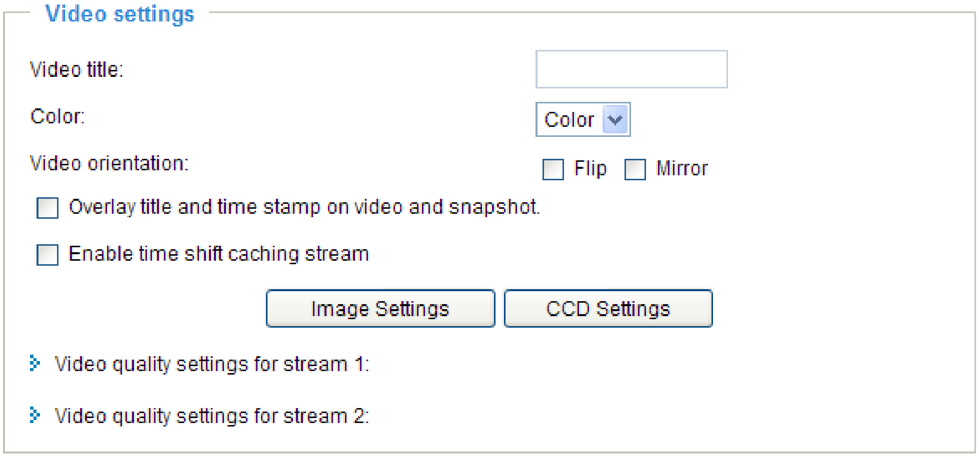
Always allow the IP address to access this device: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.



Audio and Video

This section explains how to cofigure the audio and video settings of the Network Camera. It is composed of the following two columns: Video Settings and Audio Settings.

Video Settings



Video title: Enter a name that will be displayed on the title bar of the live video.



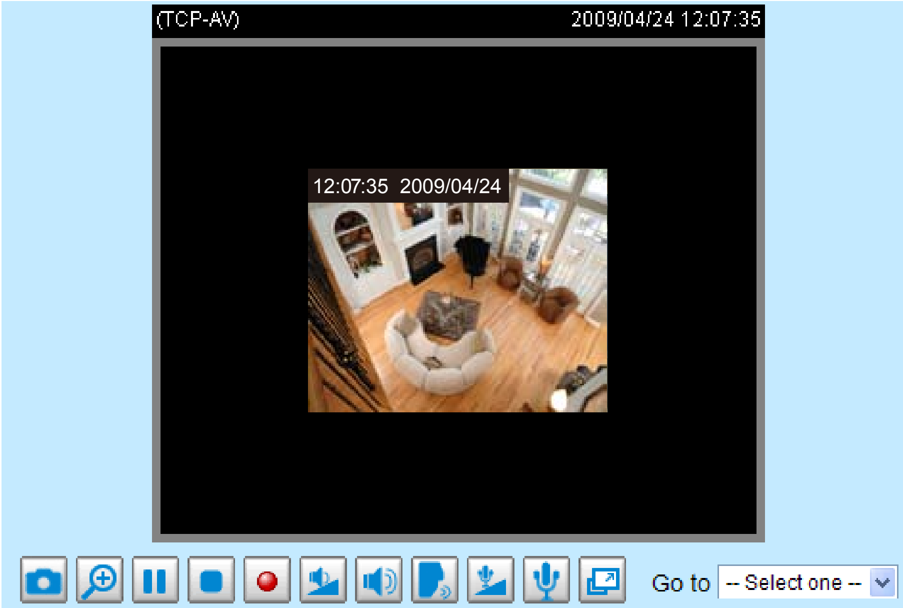
Color: Select to display color or black/white video streams.

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling) to correct the image orientation.

Overlay title and time stamp on video: Select this option to place the video title and time on the video streams.

Note that when the frame size is set to 176 x 144 as shown in the picture below, only the time will be stamped on the video streams.



Enable time shift caching stream **Advanced Mode**: Check this item to enable the time shift cache stream on the Network Camera, which will stores video in the camera's embedded memory for a period of time depending on the cache memory of each Network Camera. This function can work seamlessly with VIVOTEK's ST7501 recording software. When an event occurs, the recording software can request time shift cache stream from the camera, which allows the user to get an earlier video data.

Image Settings **Advanced Mode**

Click **Image Settings** to open the Image Settings page. On this page, you can tune the Brightness, Saturation, Contrast, and Sharpness for the video.



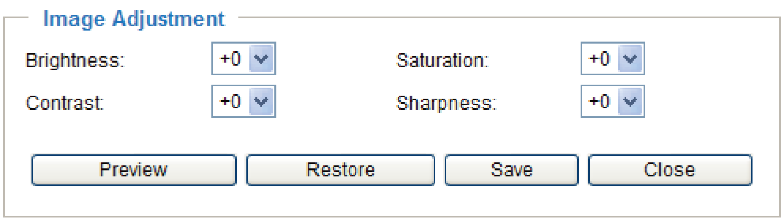


Image Adjustment

■ Brightness: Adjust the image brightness level, which ranges from -5 to +5. The default value is set to 0.

■ Saturation: Adjust the image saturation level, which ranges from -5 to +5. The default value is set to 0.

■ Contrast: Adjust the image contrast level, which ranges from -5 to +5. The default value is set to 0.

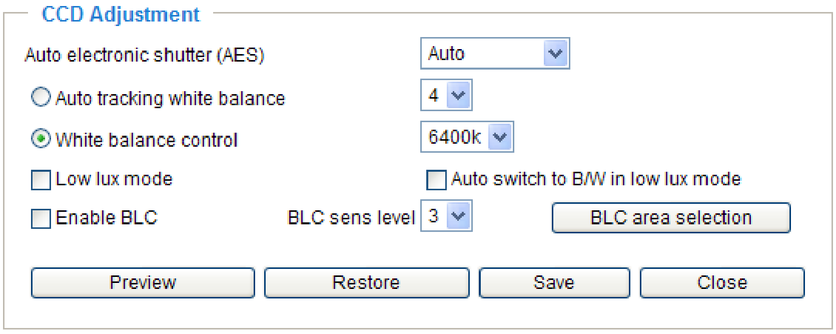
■ Sharpness: Adjust the image sharpness level, which ranges from -3 to +3. The default value is set to +3.

You can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting and click **Close** to exit the page.

CCD Adjustment Advanced Mode

Click **CCD settings** to open the CCD Adjustment page. On this page, you can set the Auto electronic shutter (AES), Auto tracking white balance, White balance control, Low lux mode, and BLC settings.





Auto electronic shutter (AES): The default iris setting of the CCD is fixed mode, and the AES option will be **1/50 (1/60)**. There are several options for AES: 1/50 (1/60), 1/100 (1/120), 1/250, 1/500, 1/1000, 1/200, and 1/4000. Faster electronic shutter would enable the Network Camera to capture fast-moving objects more clearly. Once the shutter is selected as Auto, the iris of the CCD will become fixed.

Auto tracking white balance: This option is usually selected when the Network Camera is placed in outdoor environments. Adjusting the 0~8 level would help the Network Camera capturing video with correct colors. The default value is set to 4.

White balance control: Select this option will disable Auto tracking white balance. This option is usually selected when the Network Camera is placed in indoor environments. The administrator can adjust the value for best color temperature: 3200k, 4000k, 4800k, 5600k, 6400k, 7200k, 8000k.

Low lux mode: Select this option would enable the Network Camera to capture clear images in poor illuminative environments.

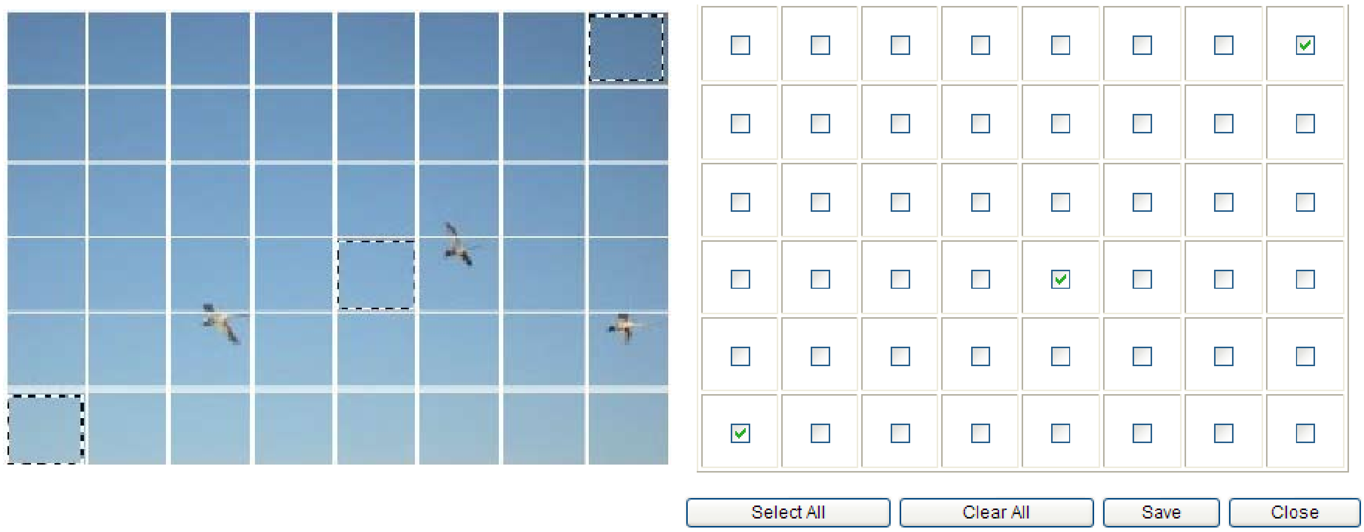
Auto switch to B/W in low lux mode: Select it to enable the Network Camera to automatically switch to B/W in low lux mode.

Enable BLC (Back Light Compensation): Select it when the object is too dark or too bright to be recognized. It will give the captured images the necessary light compensation.

BLC sens level: Select 0~7 level to adjust the sensitivity of BLC detection. Select a higher level will raise the sensitivity. The default value is set to 3.

BLC area selection: Click this button to open an area selection window. As the window shown below, the video will be divided into 48 rectangle areas equally. Check some of the areas to enable BLC. Note that if no area is selected, the Enable BLC option would be of no use.

The picture below illustrates the corresponding areas of the selection window. You can click **Select All** to check all the areas in the window, or click **Clear All** to do vice versa. When completed with the settings on this page, click **Save** to take effect and click **Close** to exit the page.



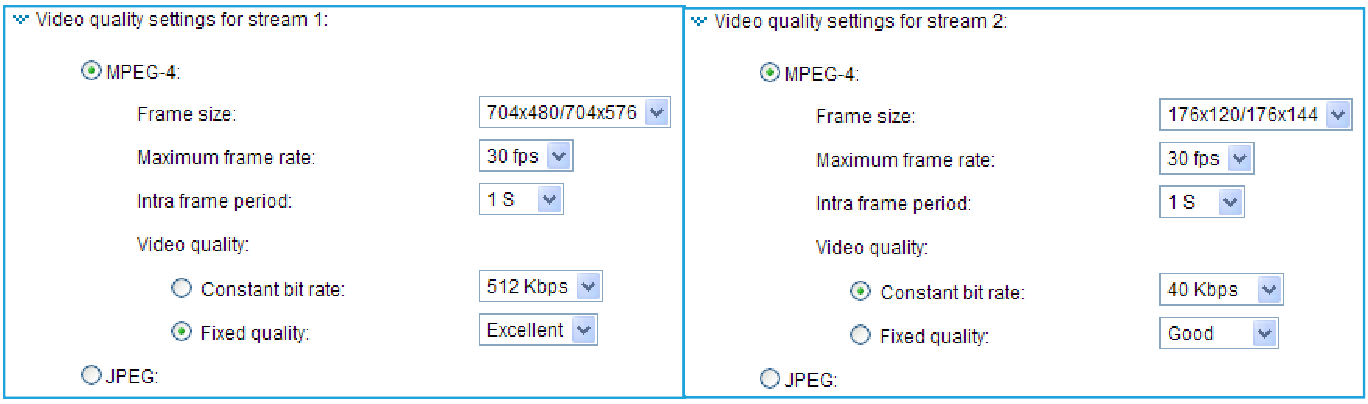
Back to the CCD Settings page, you can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to take effect and click **Close** to exit the page.

Video quality settings for stream 1 / stream 2 Advanced Mode

The Network Camera offers two choices of video compression standards for real-time viewing: MPEG-4 and MJPEG.

Click the items to display the detailed configuration settings. You can set up two seperate streams for the Network Camera for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers.

If **MPEG-4** mode is selected, it is streamed in RTSP protocol.



There are four parameters provided in MPEG-4 mode which allow you to adjust the video performance:

■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions:

	NTSC	PAL
	704 x 480	704 x 576
CIF	352 x 240	352 x 288
QCIF	176 x 120	176 x 144

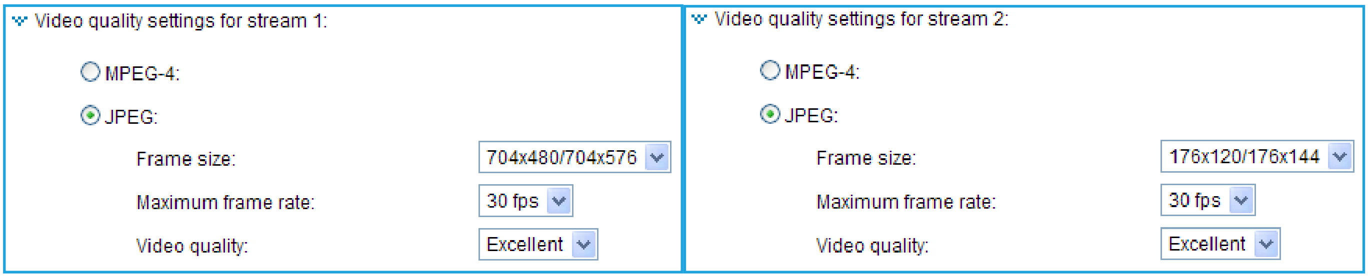
■ Maximum frame rate
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video quality. The frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. You can also select **Customize** and manually enter a value.

■ Intra frame period
Determine how often to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality
A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if **Constant bit rate** is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, and 4Mbps. You can also select **Customize** and manually enter a value.

On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

If **JPEG** mode is selected, the Network Camera continuously sends JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client.



There are three parameters provided in MJPEG mode to control the video performance:

■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions:

	NTSC	PAL
	704 x 480	704 x 576
CIF	352 x 240	352 x 288
QCIF	176 x 120	176 x 144

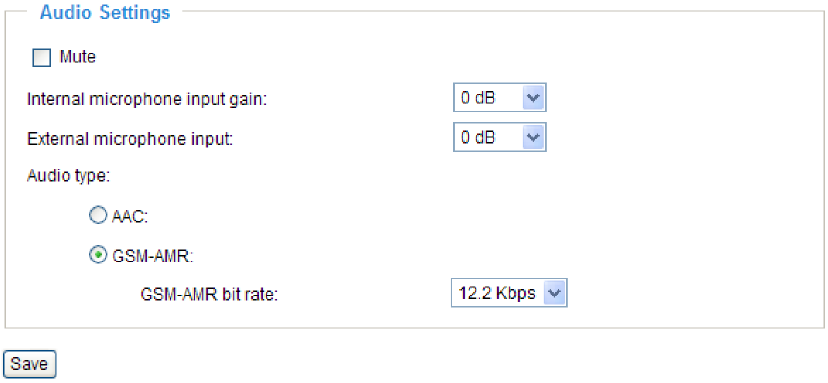
■ Maximum frame rate
This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality. The frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. You can also select **Customize** and manually enter a value.

■ Video quality
The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

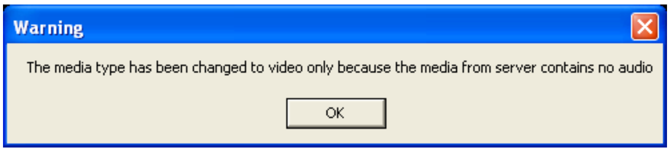
NOTE

► *Video quality and fixed quality refers to the **compression rate**, so a lower value will produce higher quality.*

Audio Settings



Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if mute mode is turned on, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, the following message is displayed:



Internal microphone input gain: Select the gain of the internal audio input according to ambient conditions. Adjust the gain from +21 db (most sensitive) ~ -33 db (least sensitive).

External microphone input: Select the gain of the external audio input according to ambient conditions. Adjust the gain from +21 db (most sensitive) ~ -33 db (least sensitive).

AAudio type: Select audio codec AAC or GSM-AMR and the bit rate.
■ AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.

■ GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable from: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps, and 12.2Kbps.

When completed with the settings on this page, click **Save** to enable the settings.

NOTE

► *The Network Camera offers two inputs to capture audio - internal microphone or external microphone. The internal/external microphone switch is located on the back panel of the Network Camera.*

Motion Detection

This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.



Follow the steps below to enable motion detection:

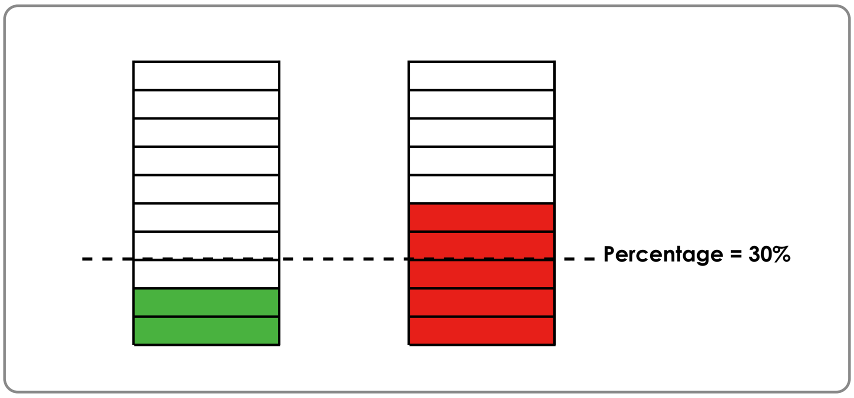
1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
   - ■ To move and resize the window, drag and drop your mouse on the window.
   - ■ To delete window, click X on the top right corner of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slider bar.
4. Click **Save** to enable the settings.
5. Select **Enable motion detection** to enable this function.

For example:



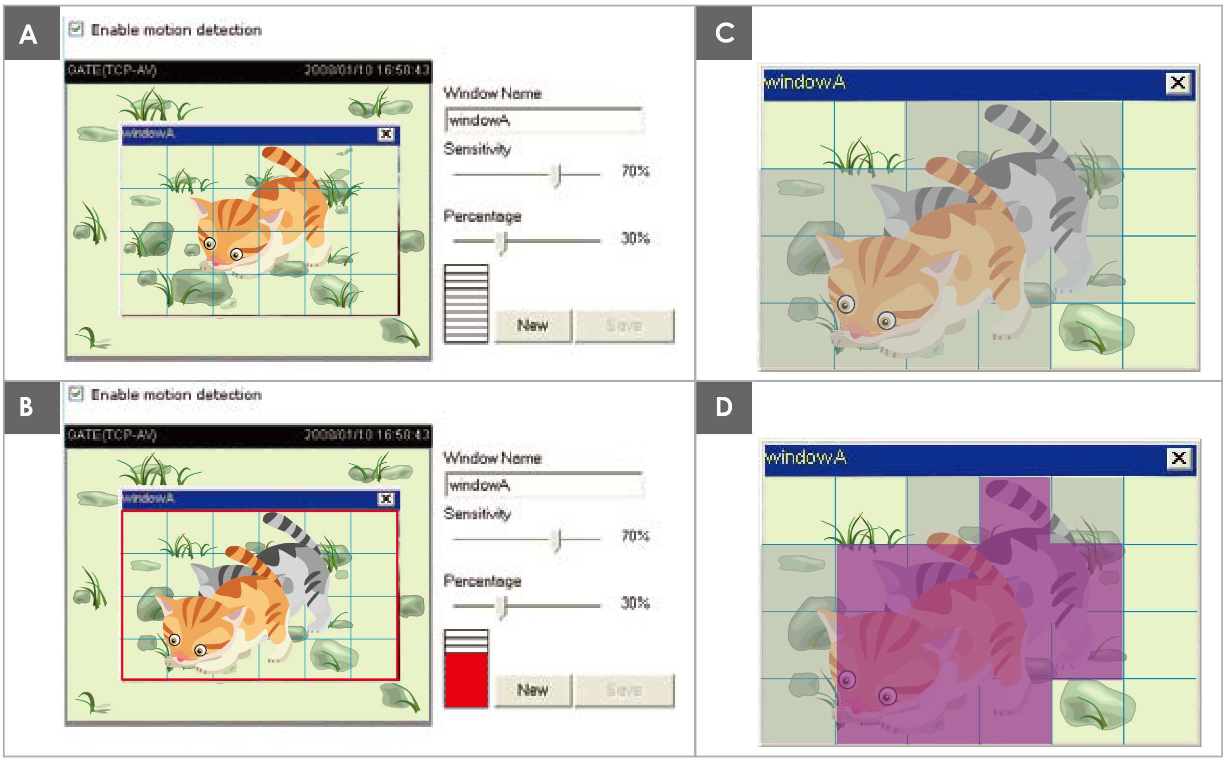
The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to set an event, please refer to Application on page 65.

A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the defined threshold.



NOTE

► *How does motion detection work?*



There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require a high level of security management, it is suggested to use higher sensitivity settings and smaller percentage values.

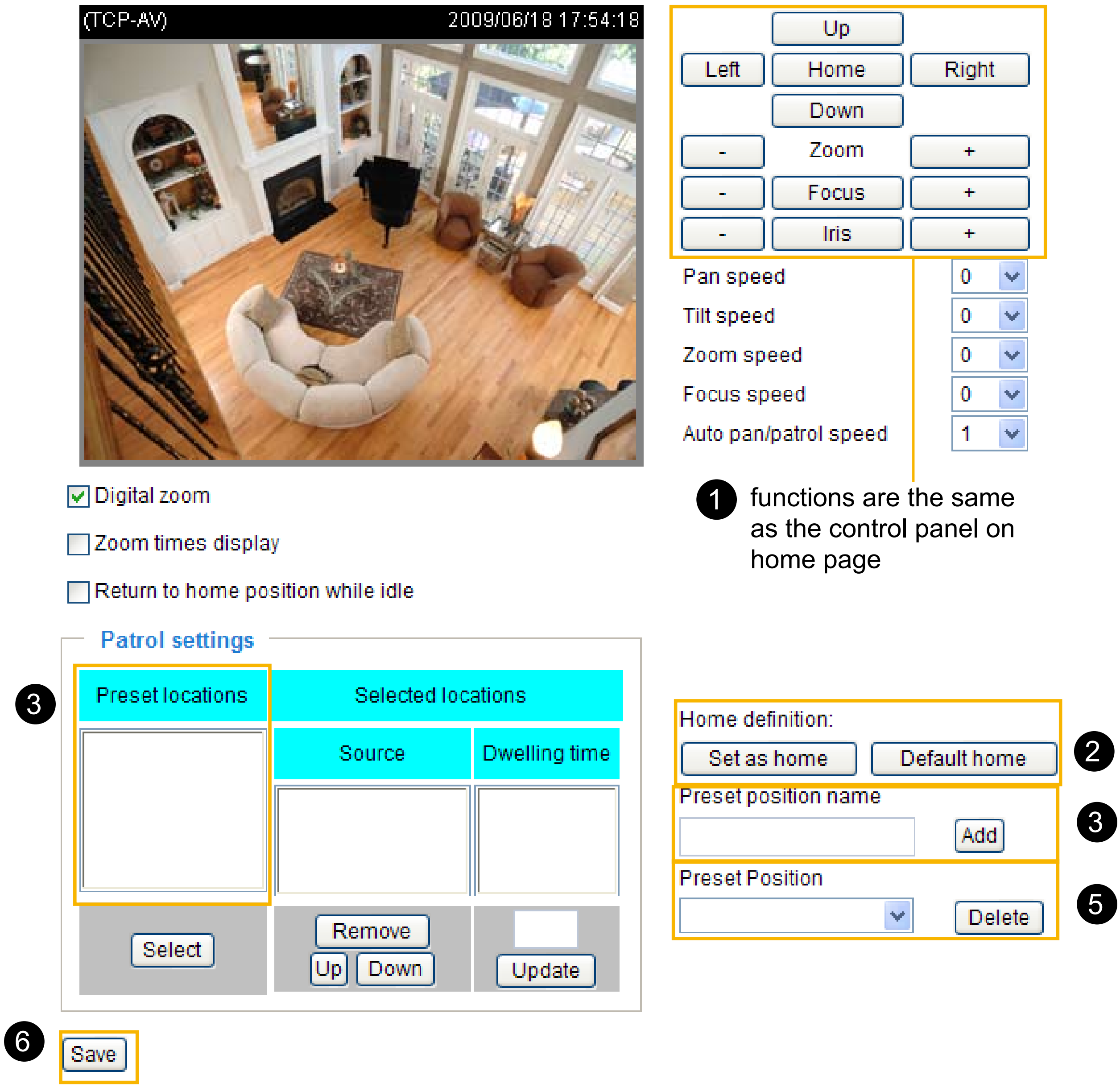
Camera Control

This section explains how to control the Network Camera's Pan/Tilt/Zoom/Focus operation via the control panel and how to preset positions.

Preset Locations

On this page, you can preset positions for the Network Camerato go to directly or patrol. A total of 128 preset positions can be configured.

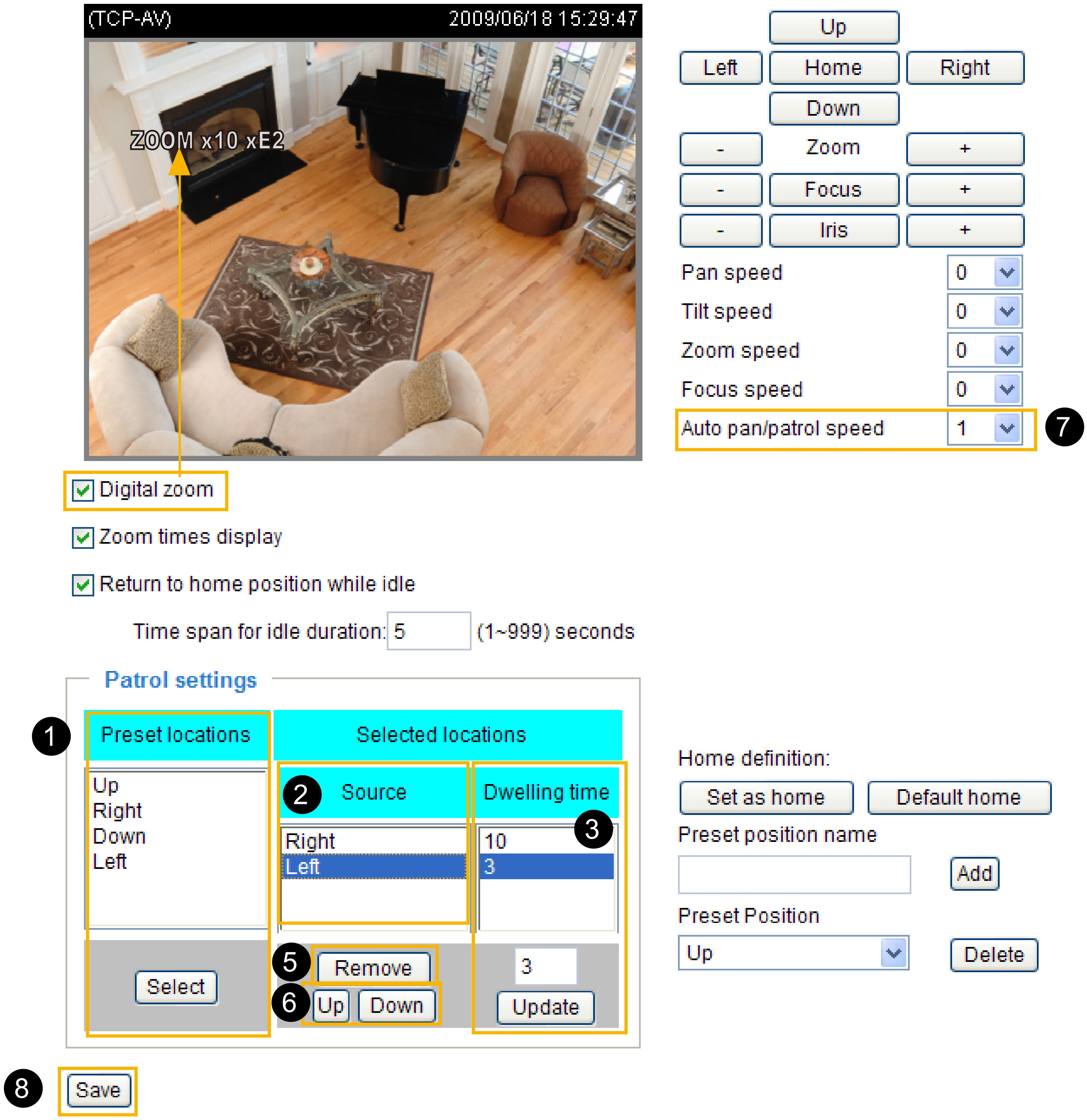
Please follow the steps below to preset a position:
1. Adjust the shooting area to a desired position using the buttons on the right side of the window.
2. Click **Set as home** or **Default home** to define your home position.
3. Enter a name for the preset position, which allows for up to forty characters. Click **Add** to enable the settings. The preset positions will be displayed under the Preset Location list on the left-hand side.
4. To add additional preset positions, please repeat step 1~3.
5. To remove a preset position from the list, select it from the drop-down list and click **Delete**.
6. Click **Save** to enable the settings.



Patrol Settings

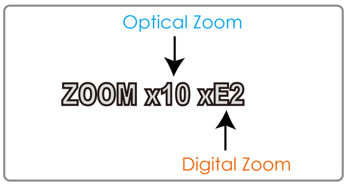
You can select preset locations for the Network Camera to patrol.
Please follow the steps below to set up a patrol schedule:

1. Click a preset location on the list and click **Select**.
2. The selected preset locations will be displayed on the **Selected locations list**.
3. Set the **Dwelling time** for the preset location during auto patrol. The default value is 10 seconds. You can also manually set a value and click **Update**.
4. Repeat step 1 and 3 to select additional preset locations.
5. If you want to delete a selected location, select it from the list and click **Remove**.
6. Select a location and click **Up** or **Down** to rearrange the patrol order.
7. Adjust the **Auto pan/patrol speed**. (1~5 seconds)
8. Click **Save** to enable the settings.



Digital Zoom
If you check this optionand click the **Save** button, the digital zoom function of CCD module will be enabled.

Zoom Times Display
If you check this item and click the **Save** button, the zoom indicator will be displayed on the screen when you zoom in/out as shown in the illustration above. Please remember to click **Save** to enable the settings.



Return to Home Position while Idle
If you select this option, the Network Camera will automatically return to the home position after idling for a specific time span. Please remember to click **Save** to enable the settings.

■ The Preset Locations will be displayed on the Home page:



■ Click **Go to**: The Network Camera will move to the preset location.
■ Click **Patrol**: The Network Camera will patrol among the selected preset positions (from right to left) for once.

Homepage Layout Advanced Mode

This section explains how to set up your own customized homepage layout.

Preview

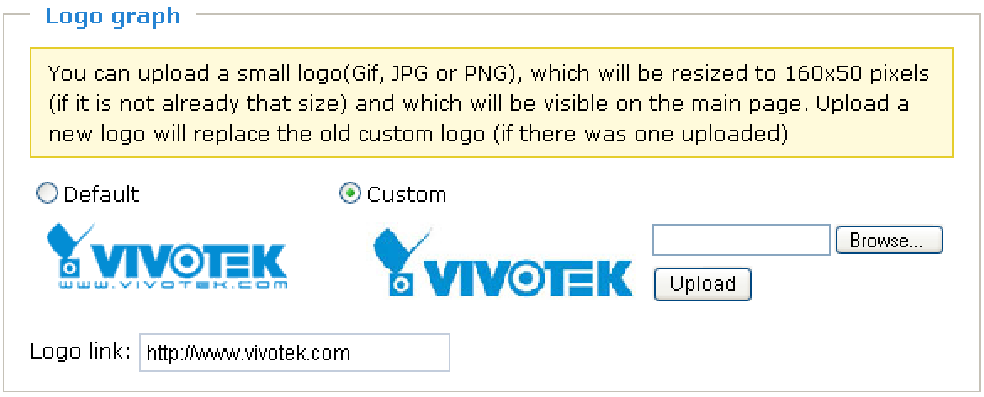
This column shows the settings of your homepage layout. You can manually select the background and font colors in Theme Options, the third column on this page. The settings will automatically show up in this Preview field. The following shows the homepage using the default settings:



■ Hide Powered by VIVOTEK: If you check this item, it will be removed from the homepage.

Logo

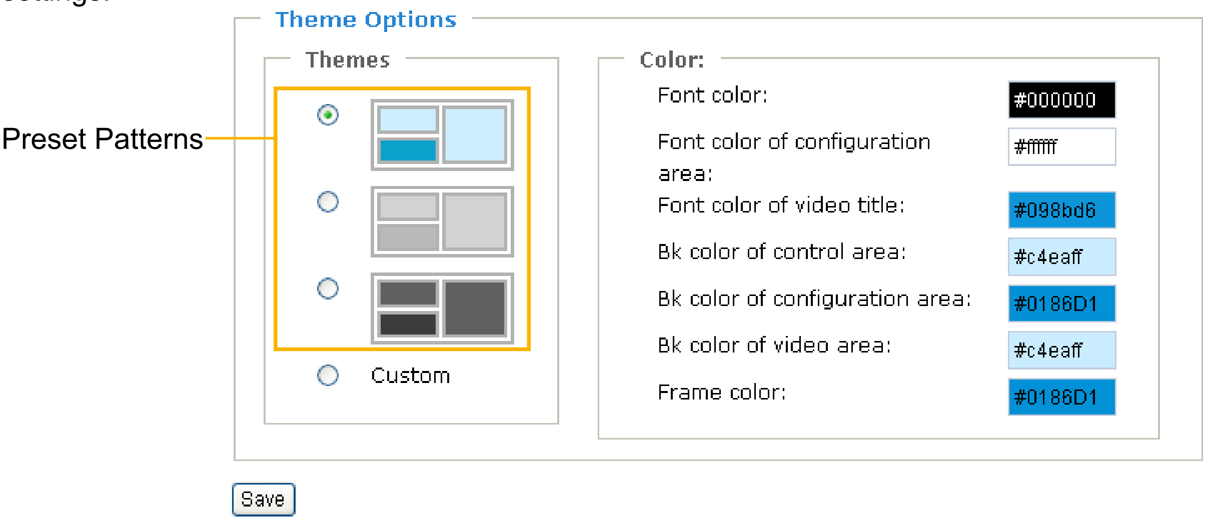
Here you can change the logo at the top of your homepage.



Follow the steps below to upload a new logo:
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

Theme Options

Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.

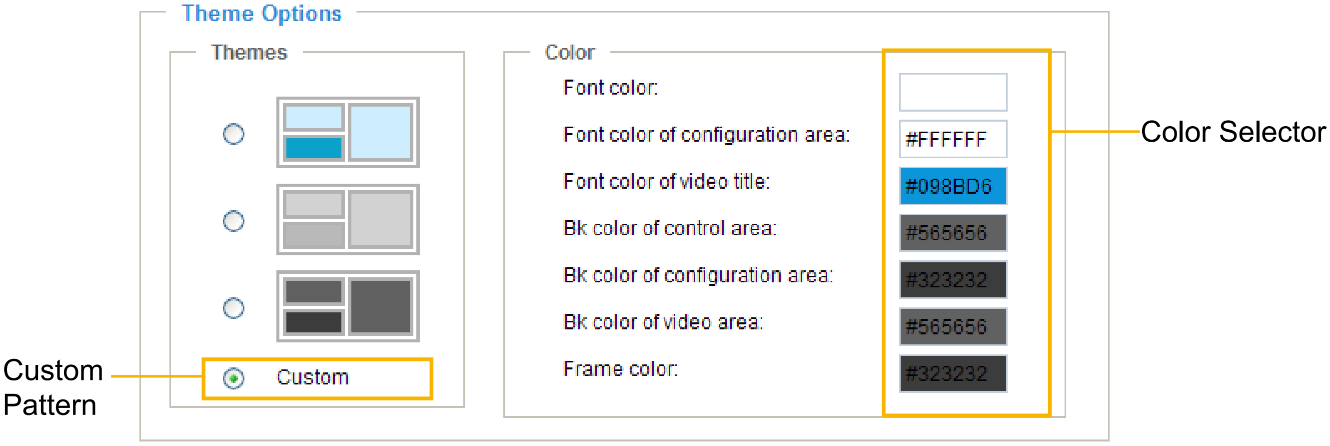




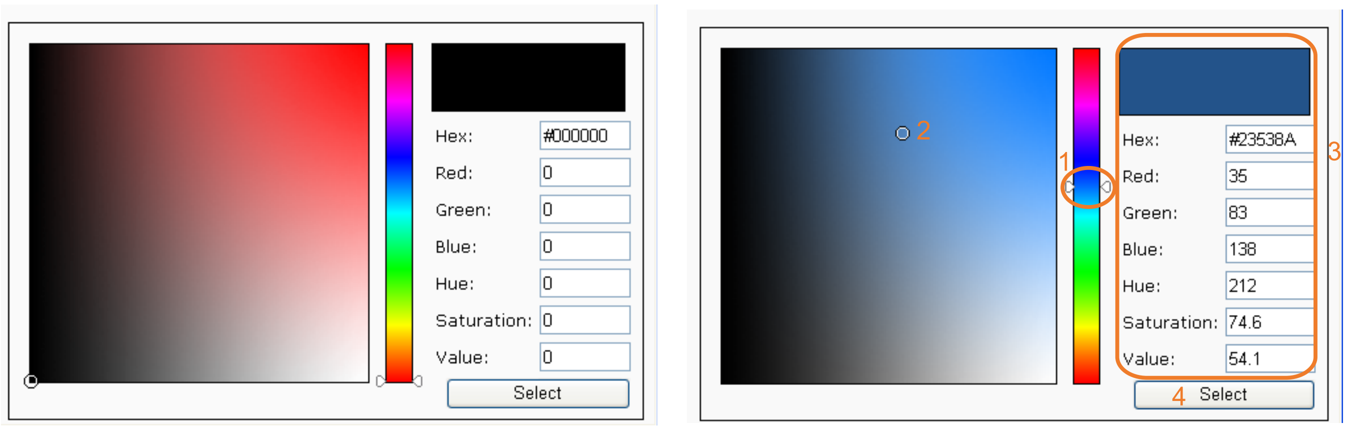




■ Follow the steps below to set up the customed homepage:
1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.



3. The palette window will pop up as shown below.

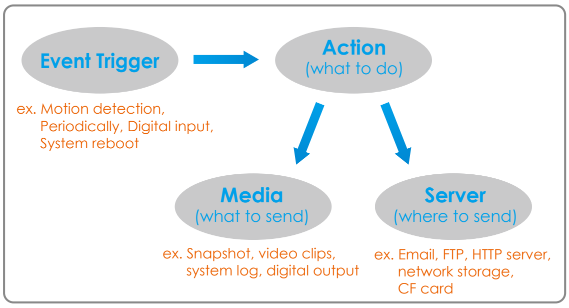


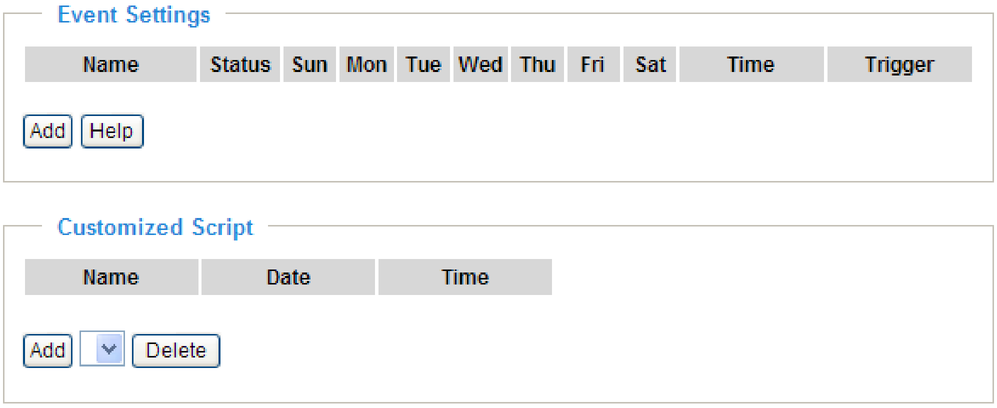
4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will show up in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

Application Advanced Mode

This section explains how to configure the Network Camera to react in response to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to a FTP server or e-mail address as notifications.

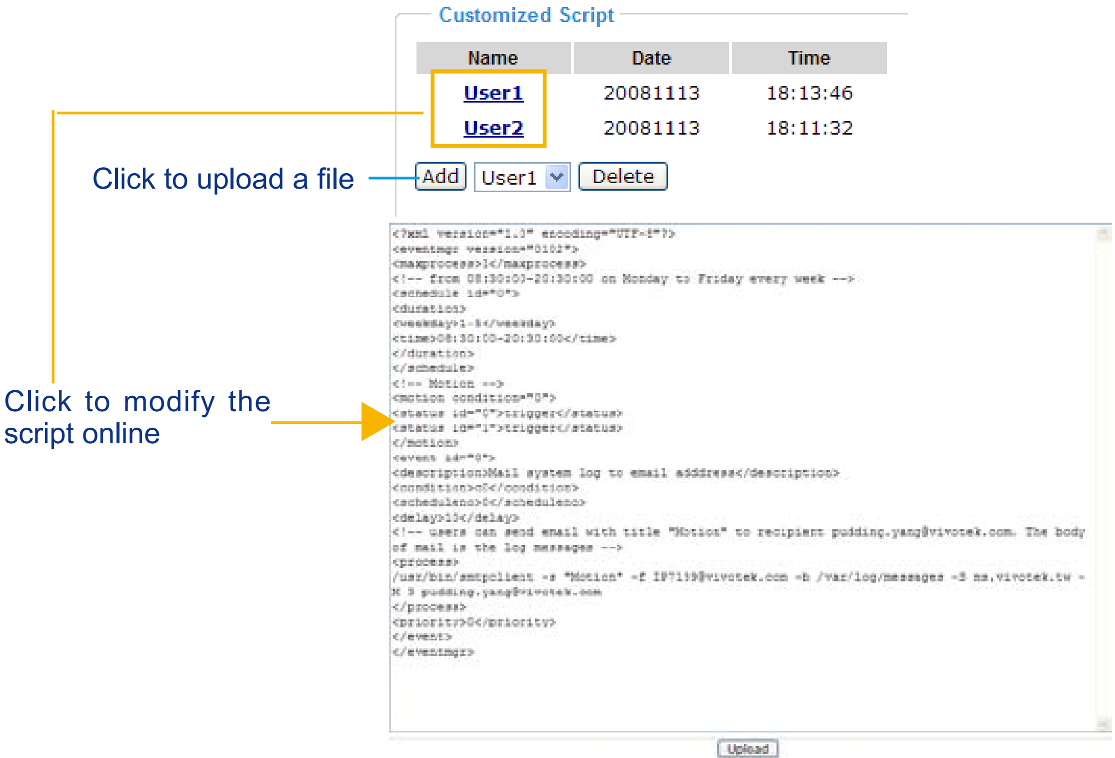
In the illustration on the right, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.





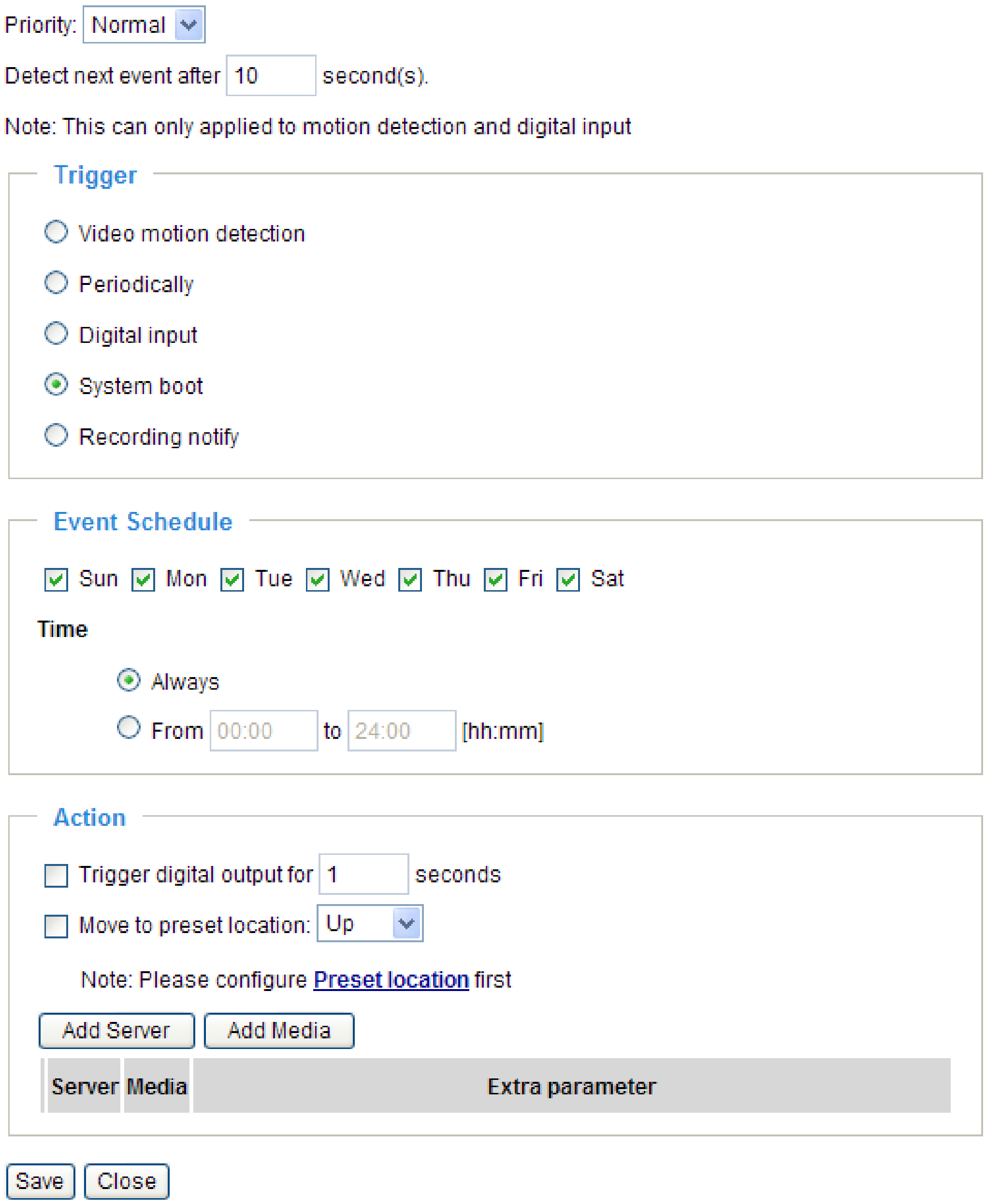
Customized Script

This function allows you to upload a sample script (.xml file) to the webpage, which will save your time on configuring the settings. Please note that there is a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will pop up. If you need more information, please ask for VIVOTEK's technical support.



Event Settings

In the **Event Settings** column, click **Add** to open the **Event Settings** page. On this page, you can arrange three elements -- Trigger, Schedule, and Action to set an event. A total of 3 event settings can be configured.



Event name: Enter a name for the event setting.

Enable this event: Select this option to enable the event setting.

Priority: Select the relative importance of this event (High, Normal, or Low). Events with a higher priority setting will be executed first.

Detect next event after ☐ seconds: Enter the duration in seconds to pause motion detection after a motion is detected.

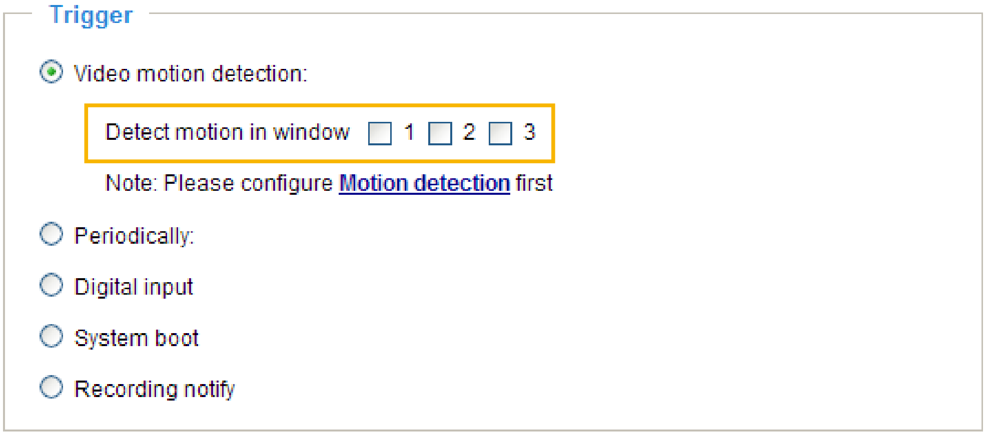
An event is an action initiated by a user-defined trigger source; it is the causal arrangement of the following three elements: Trigger, Event Schedule, and Action.

Trigger

This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.
There are several choices of trigger sources as shown below. Select the items to display the detailed configuration options.

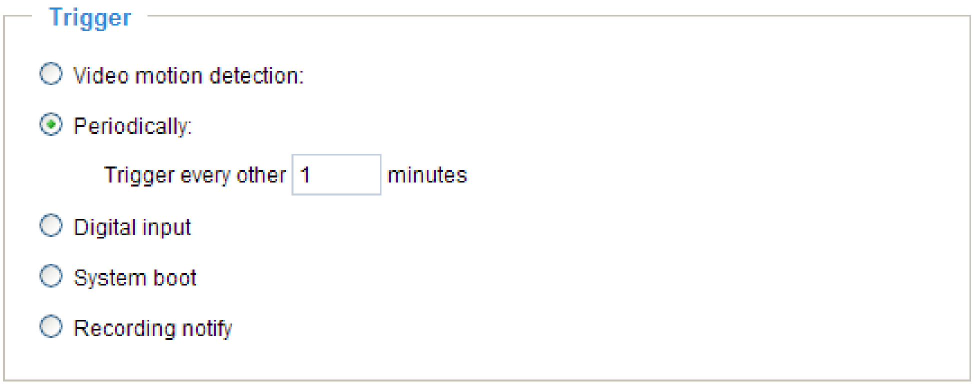
■ Video motion detection

This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection on page 57 for details.



■ Periodically

This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.



■ Digital input

This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound and light, etc.

■ System boot

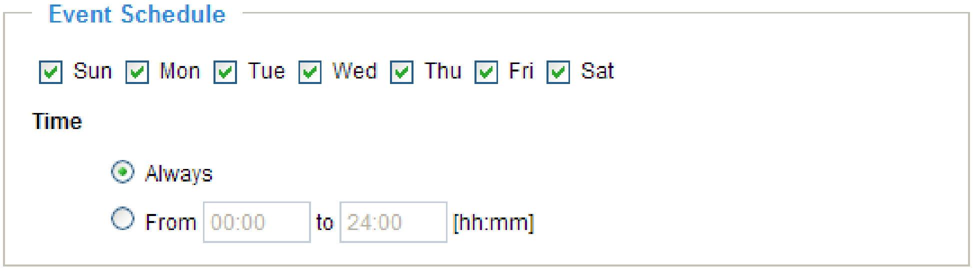
This option triggers the Network Camera when the power to the Network Camera is disconnected.

■ Recording notify

This option allows the Network Camera to trigger when the recording disk is full or when recording starts to rewrite older data. If you want receive **Recording notify message**, please refer to page 76 for detailed information.

Event Schedule

Specify the period for the event.

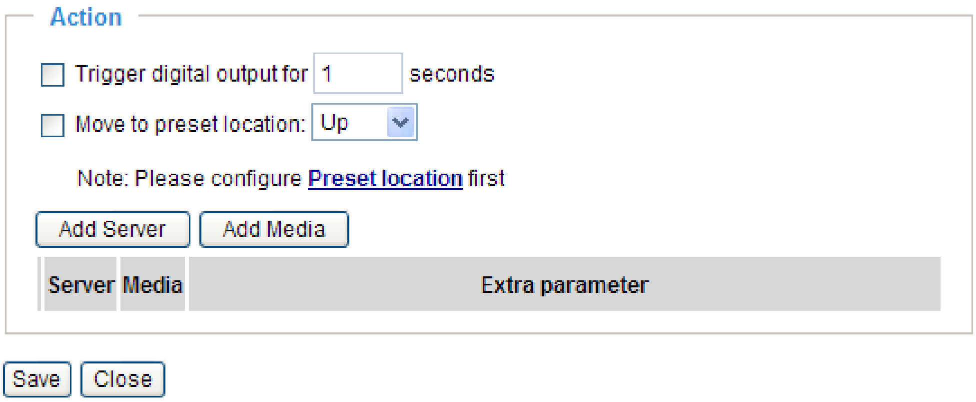


■ Select the days of the week.

■ Select the recording schedule in 24-hr time format.

Action

Define the actions to be performed by the Network Camera when a trigger is activated.



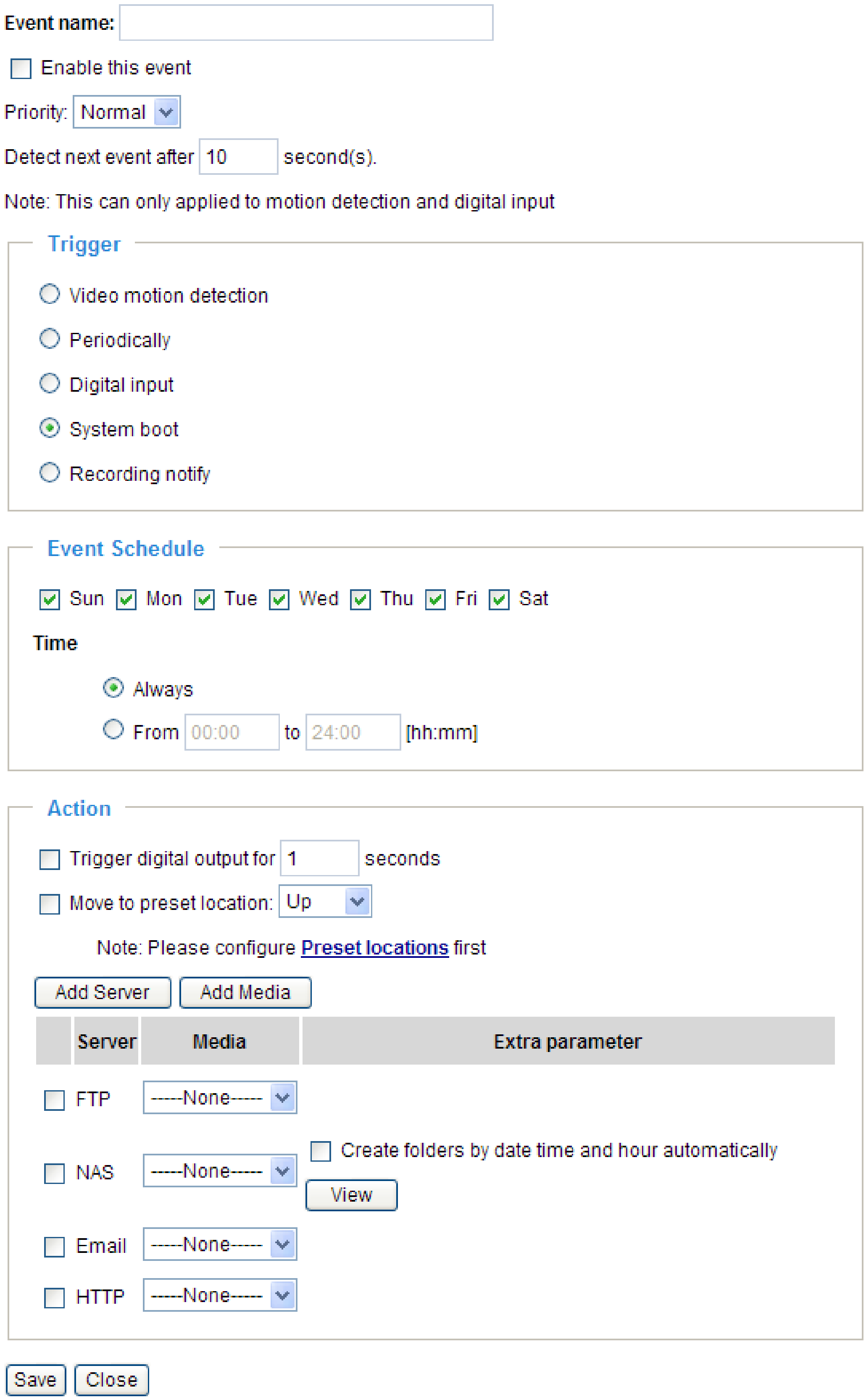
■ Trigger digital output for ☐ seconds
Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.

■ Move to preset location
Select this option, the Network Camera will move to the preset location when a trigger is activated. Please setup the preset locations first. Please refer to Preset Locations on page 59 for detailed information.

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated.

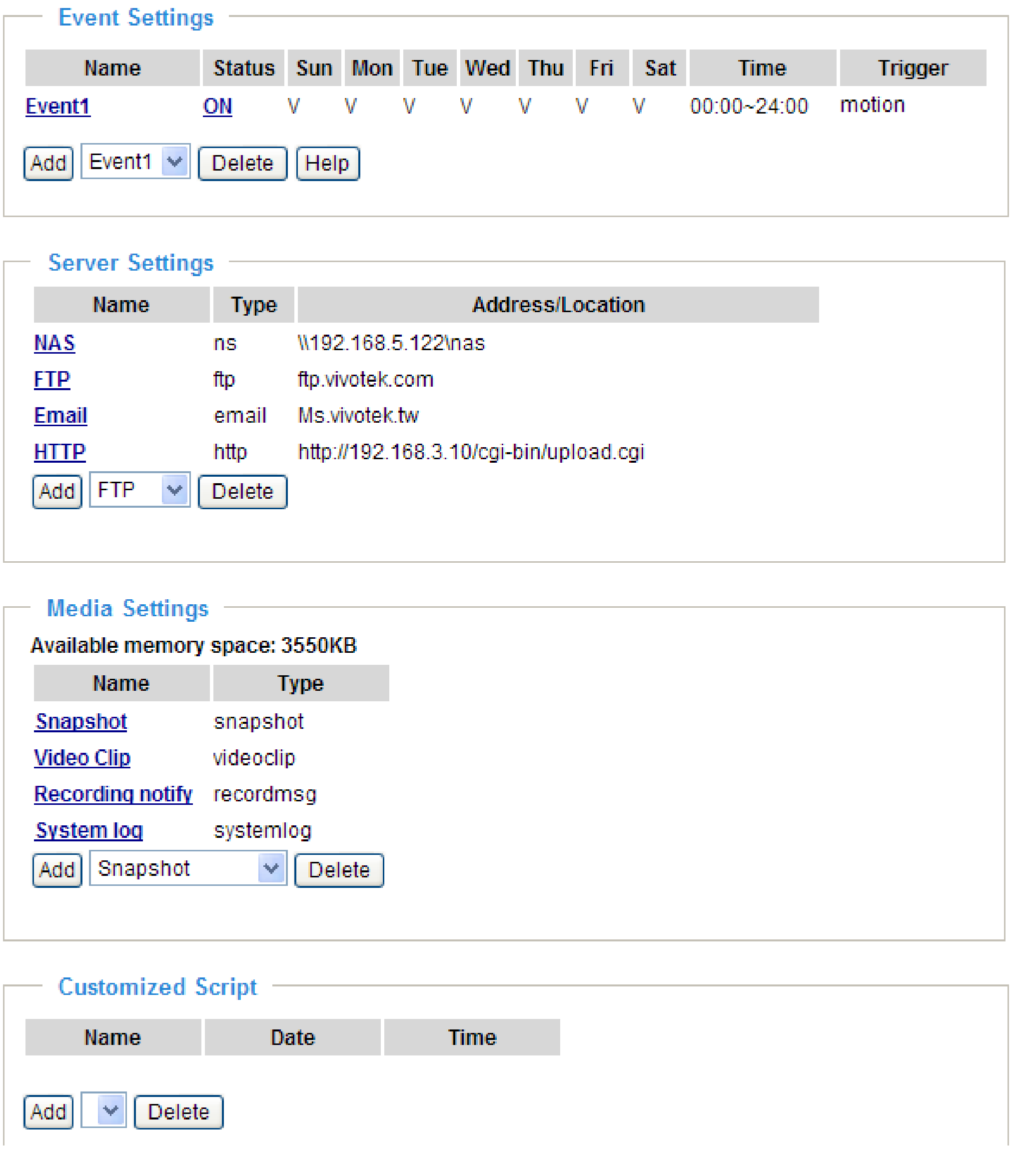
■ Add Server / Add Media
Click **Add Server** to configure Server Settings. For more information, please refer to Server Settings on page 71.
Click **Add Media** to configure Media Settings. For more information, please refer to Media Settings on page 74.

Here is an example of Event Settings page:



When completed, click **Save** to enable the settings and click **Close** to exit Event Settings page. The new event settings / server settings / media settings will appear in the event drop-down list on the Application page.

Here is an example of Application page with an event setting:



When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will automatically send snapshots via e-mail.

If you want to stop the event trigger, you can click **ON** to turn it to **OFF** status or click **Delete** to remove the event setting.

To remove a server setting from the list, select a server name from the drop-down list and click **Delete**. Note that only when the server setting is not being applied to an event setting can it be deleted.

To remove a media setting from the list, select a media name from the drop-down list and click **Delete**. Note that only when the media setting is not being applied to an event setting can it be deleted.

Server Settings

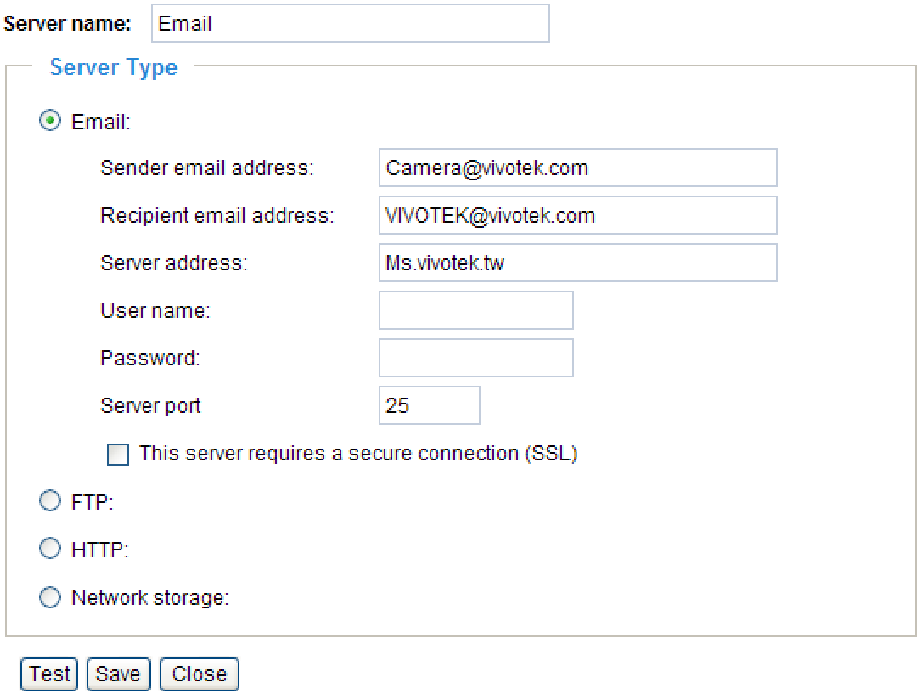
Click **Add Server** on Event Settings page to open the Server Setting page. On this page, you can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

Server name: Enter a name for the server setting.

Server Type

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.

Email: Select to send the media files via email when a trigger is activated.



■ Sender email address: Enter the email address of the sender.

■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

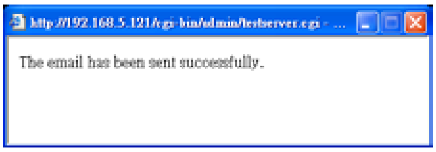
■ User name: Enter the user name of the email account if necessary.

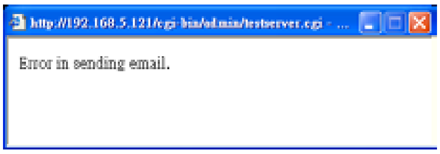
■ Password: Enter the password of the email account if necessary.

■ Server port: The default mail server port is set to 25. You can also manually set another port.

If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

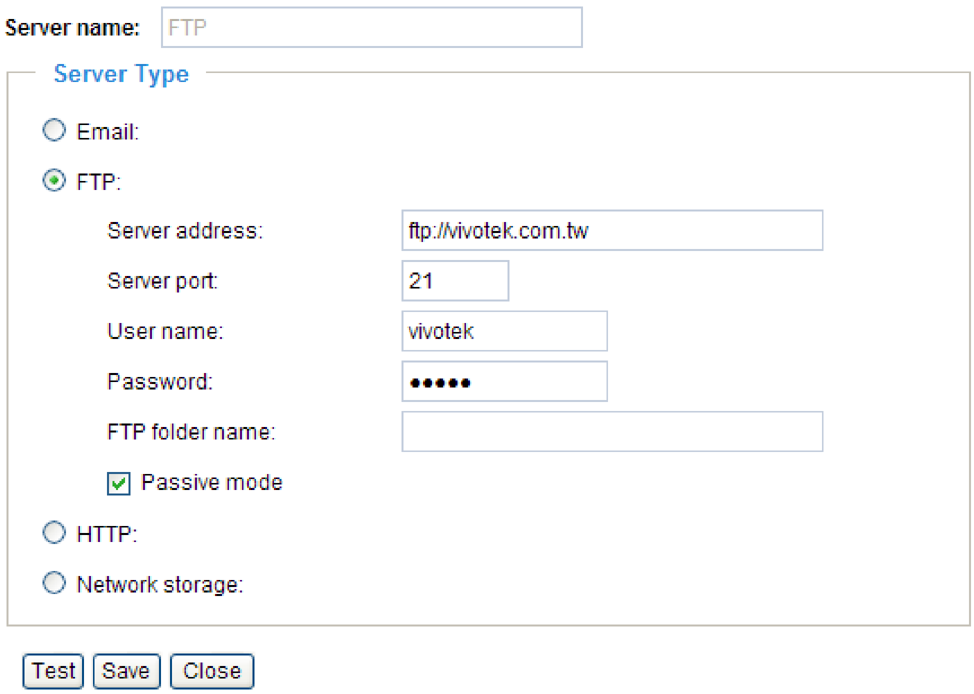
To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.





Click **Save** to enable the settings, then click **Close** to exit the page.

FTP: Select to send the media files to an FTP server when a trigger is activated.



■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port
By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.

■ User name: Enter the login name of the FTP account.

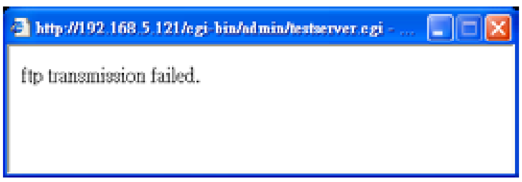
■ Password: Enter the password of the FTP account.

■ Remote folder name
Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will create one on the FTP server.

■ Passive mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

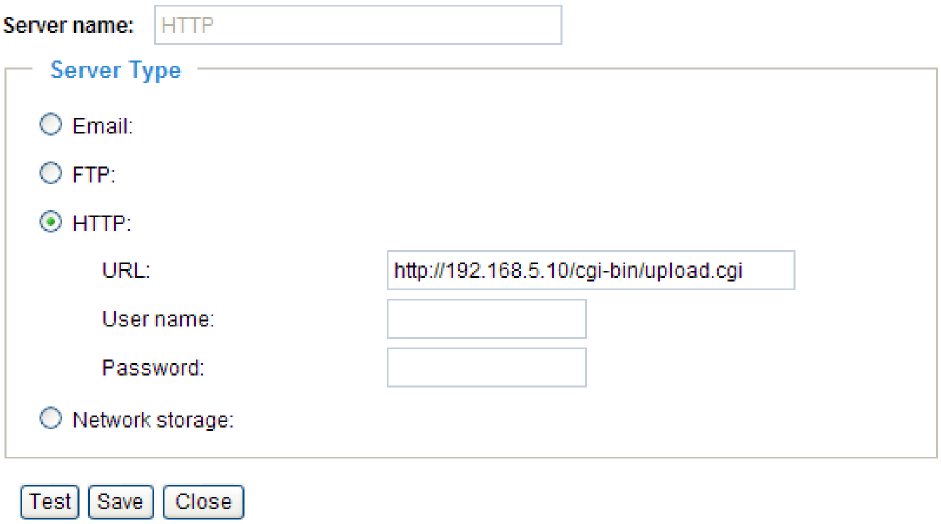
To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.





Click **Save** to enable the settings, then click **Close** to exit the page.

HTTP: Select to send the media files to an HTTP server when a trigger is activated.

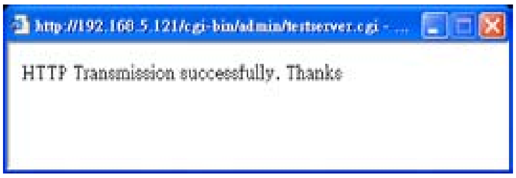


■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

■ Password: Enter the password if necessary.

To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If successful, you will receive a test.txt file on the HTTP server.



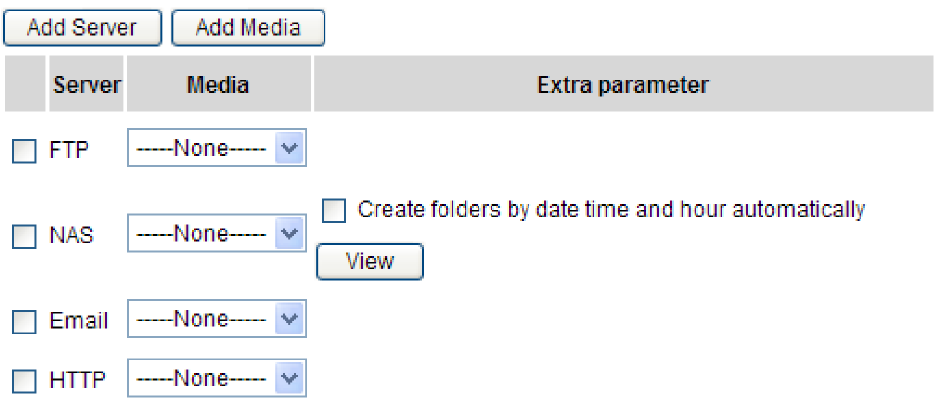


Click **Save** to enable the settings, then click **Close** to exit the page.

Network storage: Select to send the media files to a network storage location when a trigger is activated. Please refer to **Network Storage Setting** on page 78 for details.

Click **Save** to enable the settings, then click **Close** to exit the page.

When completed, the new server settings will automatically be displayed on the Event Settings page. For example:



Media Settings

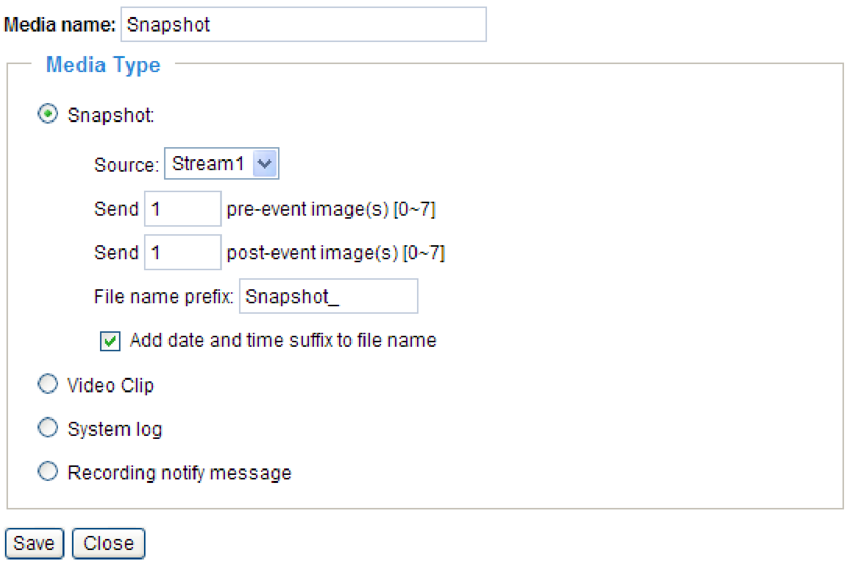
Click **Add Media** on the Event Settings page to open the Media Settings page. On this page, you can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured.

Media name: Enter a name for the media setting.

Media Type

There are three choices of media types available: Snapshot, Video clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.

Snapshot: Select to send snapshots when a trigger is activated.

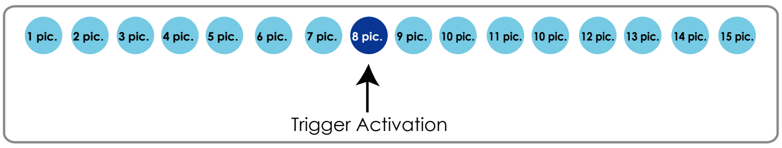


■ Source: Select to take snapshots from stream 1 or stream 2.

■ Send ☐ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

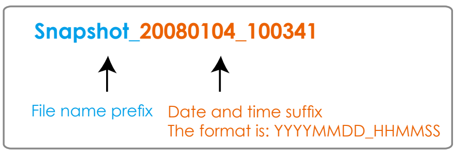
■ Send ☐ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.



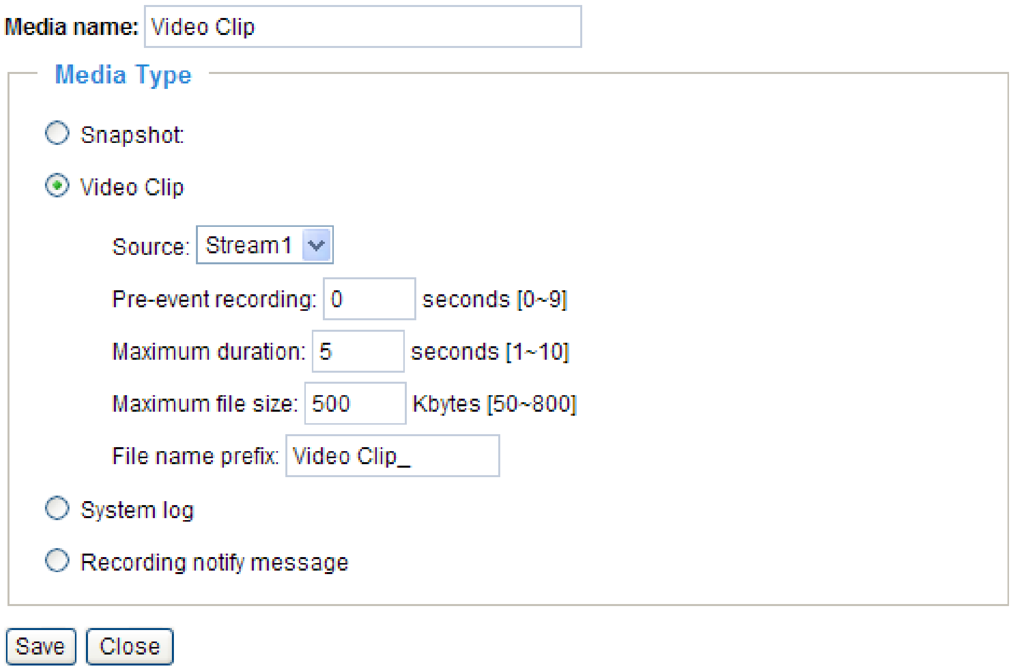
■ File name prefix
Enter the text that will be appended to the front of the file name.

■ Add date and time suffix to the file name
Select this option to add a date/time suffix to the file name.
For example:



Click **Save** to enable the settings, then click **Close** to exit the page.

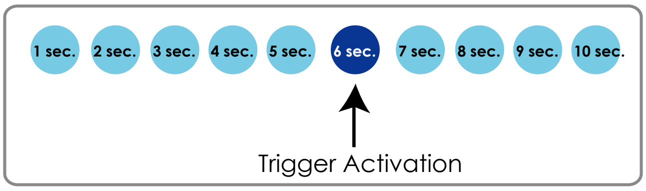
Video clip: Select to send video clips when a trigger is activated.



■ Source: Select to record video clips from stream 1 or stream 2.

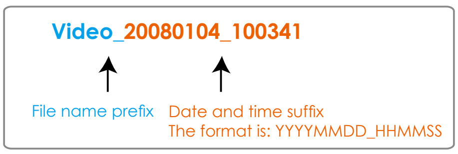
■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ Maximum duration
Specify the maximum recording duration in seconds. Up to 10 seconds can be set.
For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



■ Maximum file size
Specify the maximum file size allowed.

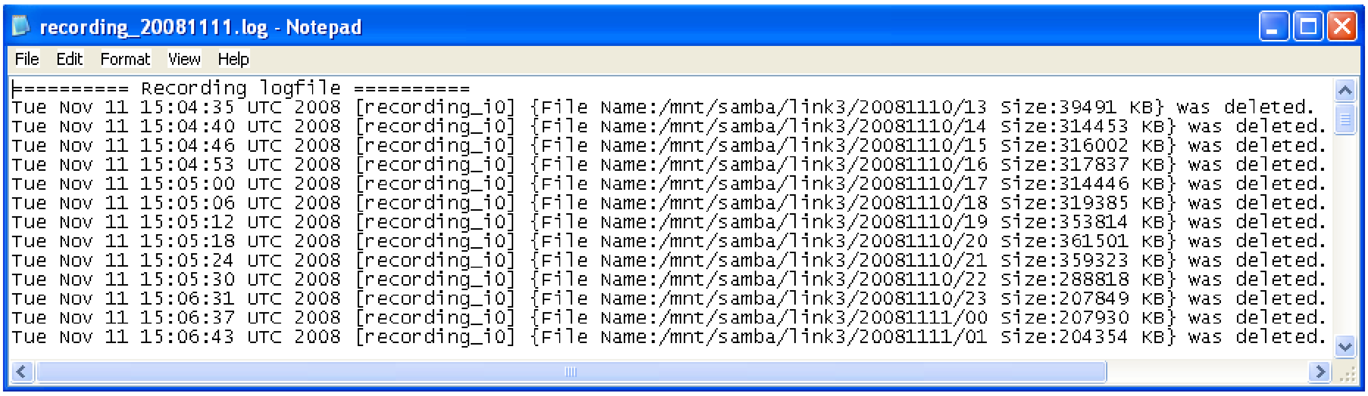
■ File name prefix
Enter the text that will appended to the front of the file name.
For example:



Click **Save** to enable the settings, then click **Close** to exit the page.

System log: Select to send a system log when a trigger is activated.
Click **Save** to enable the settings, then click **Close** to exit the page.

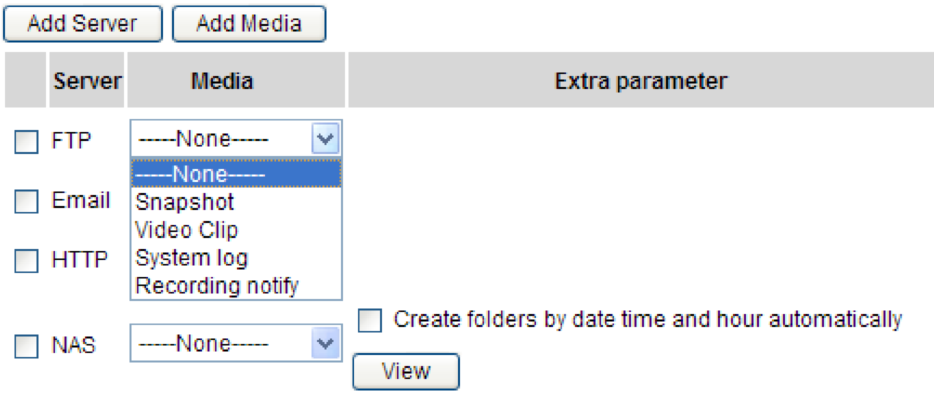
Recording notify message: Select to send a recording notification message when a trigger is activated. The following is an example of a recording notification message (.txt file), which shows a list of deleted previously-recorded data due to cycle recording.




```
========== Recording logfile ==========
Tue Nov 11 15:04:35 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/13 size:39491 KB} was deleted.
Tue Nov 11 15:04:40 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/14 size:314453 KB} was deleted.
Tue Nov 11 15:04:46 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/15 size:316002 KB} was deleted.
Tue Nov 11 15:04:53 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/16 size:317837 KB} was deleted.
Tue Nov 11 15:05:00 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/17 size:314446 KB} was deleted.
Tue Nov 11 15:05:06 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/18 size:319385 KB} was deleted.
Tue Nov 11 15:05:12 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/19 size:353814 KB} was deleted.
Tue Nov 11 15:05:18 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/20 size:361501 KB} was deleted.
Tue Nov 11 15:05:24 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/21 size:359323 KB} was deleted.
Tue Nov 11 15:05:30 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/22 size:288818 KB} was deleted.
Tue Nov 11 15:06:31 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081110/23 size:207849 KB} was deleted.
Tue Nov 11 15:06:37 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081111/00 size:207930 KB} was deleted.
Tue Nov 11 15:06:43 UTC 2008 [recording_io] {File Name:/mnt/samba/link3/20081111/01 size:204354 KB} was deleted.
```

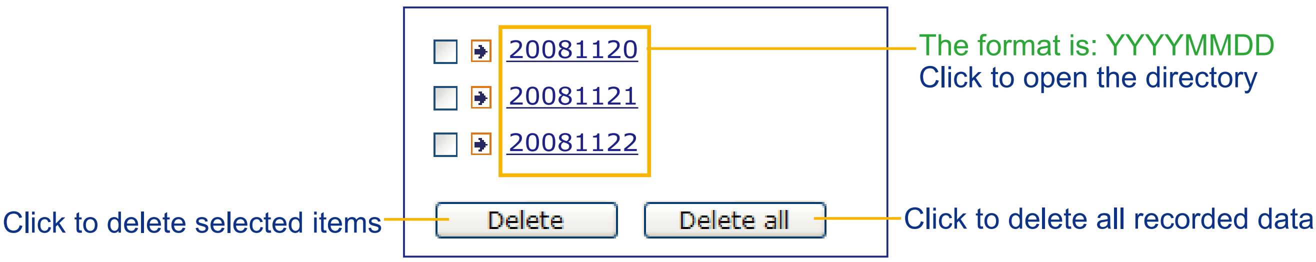
When completed, click **Save** to enable the settings and click **Close** to exit this page. The new media settings will appear on the Event Settings page.

You can continue to select a server and media type for the event.



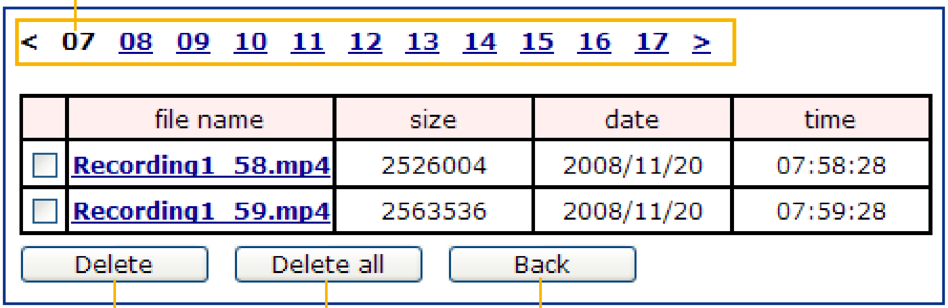
■ Create folders by date, time, and hour automatically: If you check this item, the system will generate folders automatically by date.

■ View: Click this button to open a file list window. This function is only for Network Storage.
The following is an example of a file destination with video clips:



Click 20081120 to open the directory:

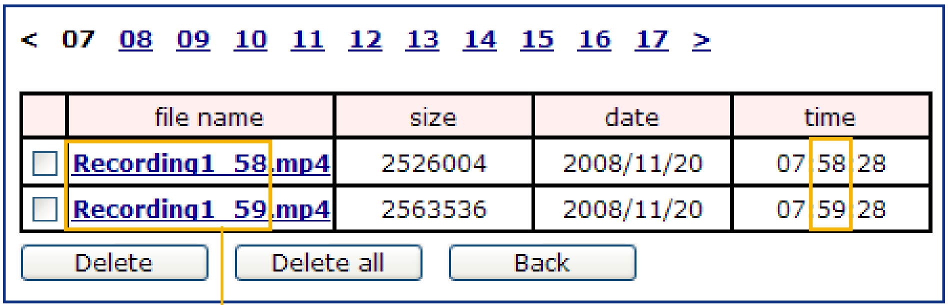
The format is: HH (24r)
Click to open the file list for that hour



Click to delete selected items

Click to go back to the previous level of the directory

Click to delete all recorded data

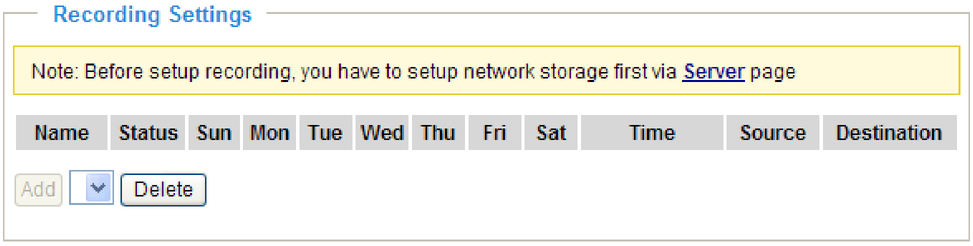


The format is: File name prefix + Minute (mm)
You can set up the file name prefix on Media Settings page.
Please refer to page 74 for detailed information.

Recording Advanced Mode

This section explains how to configure the recording settings for the Network Camera.

Recording Settings



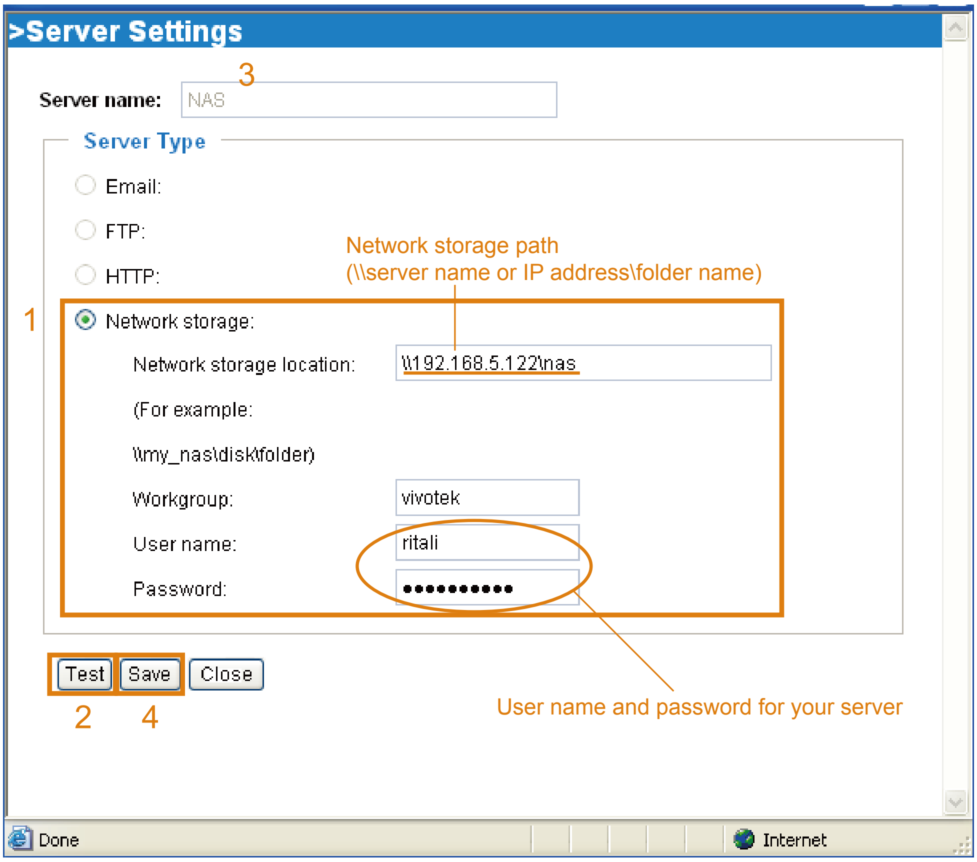
NOTE

► *Before setting up this page, please set up the Network Storage on the Server Settings page first.*

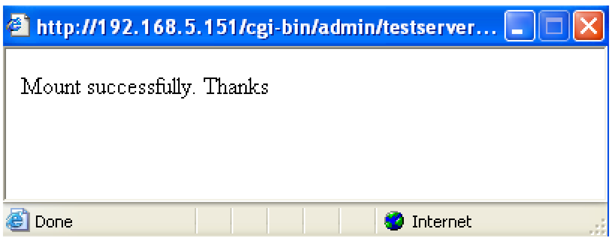
Network Storage Setting

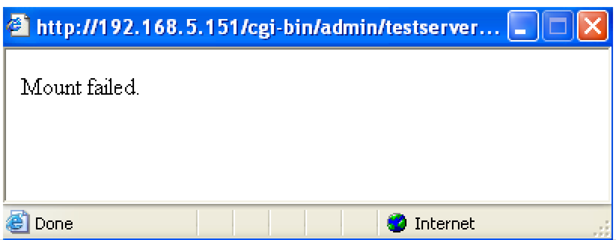
Click Server to open the Server Settings page and follow the steps below to set up:

1. Fill in the information for your server.
   For example:

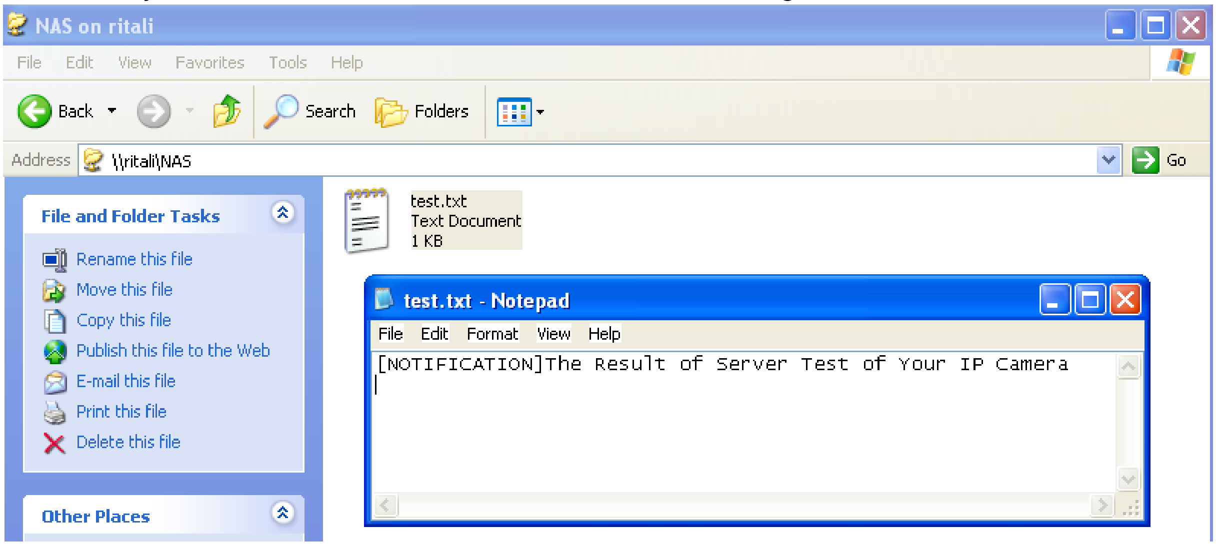


2. Click **Test** to check the setting. The result will be shown in the pop-up window.





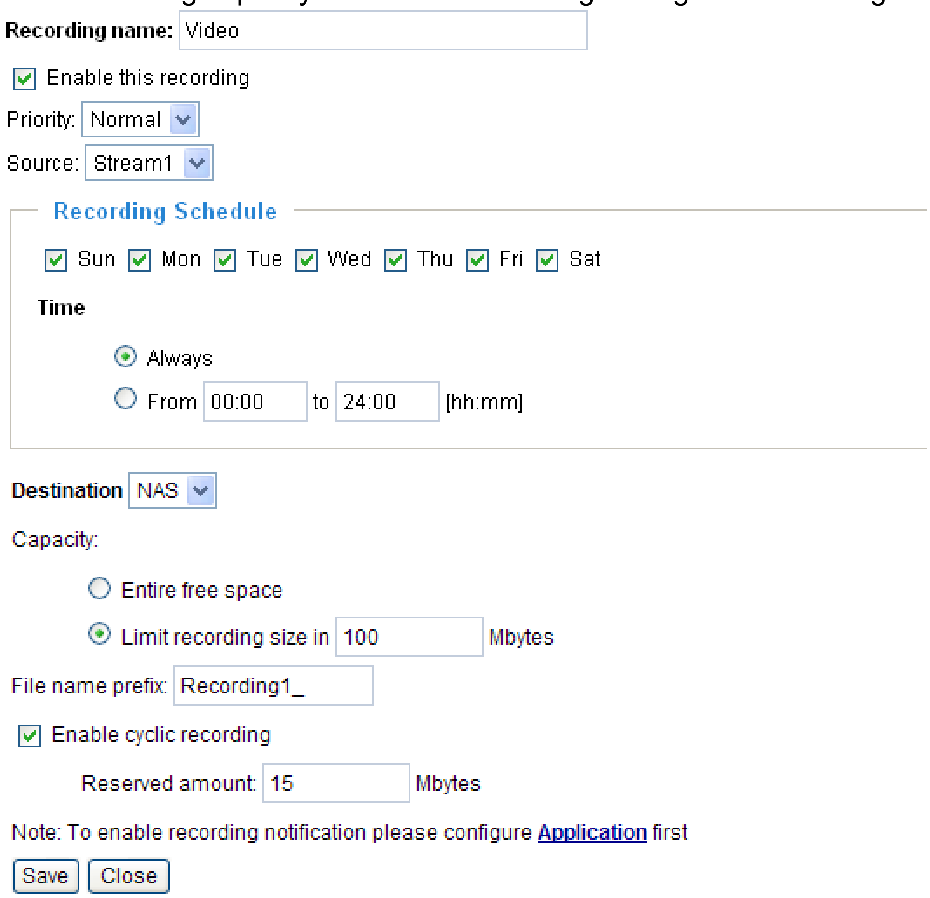
If successful, you will receive a test.txt file on the network storage server.



3. Enter a server name.
4. Click **Save** to complete the settings and click **Close** to exit the page.

Recording Settings

Click **Add** to open the recording setting page. On this page, you can define the recording source, recording schedule and recording capacity. A total of 2 recording settings can be configured.



Recording name: Enter a name for the recording setting.

Enable this recording: Select this option to enable video recording.

Priority: Select the relative importance of the recording setting (High, Normal, and Low).

Source: Select the recording source (stream 1 or stream 2).

Recording Schedule: Specify the recording duration.

■ Select the days of the week.

■ Select the recording start and end times in 24-hr time format.

Destination: You can select the network storage to store the recorded video files.

Capacity: You can choose either the “entire free space available” or “limit the recording size”. The recording size limit must be larger than the reserved amount for cyclic recording.

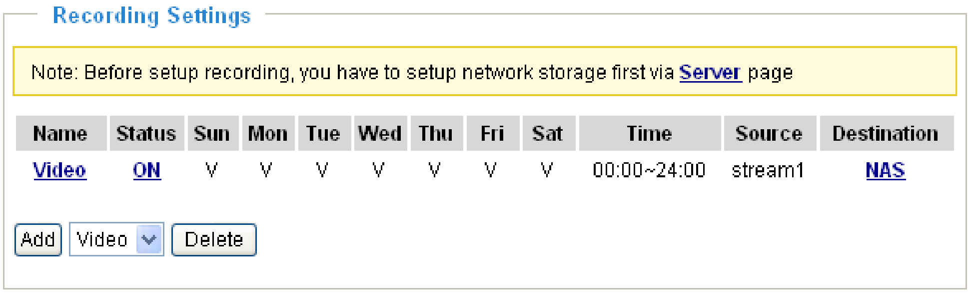
File name prefix: Enter the text that will be appended to the front of the file name.

Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for cyclic recording to prevent malfunction. This value must be larger than 15 MBytes.

If you want to enable recording notification, please click **Application** to set up. Please refer to **Trigger > Recording notify** on page 67 for detailed information.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the Network Storage. The new recording name will appear in the drop-down list on the recording page as shown below.

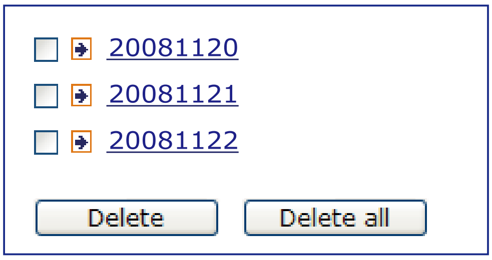
To remove a recording setting from the list, select a recording name from the drop-down list and click **Delete**.



■ Click **Video** **(Name)**: Opens the Recording Settings page to modify.

■ Click **ON** **(Status)**: The Status will become **OFF** and stop recording.

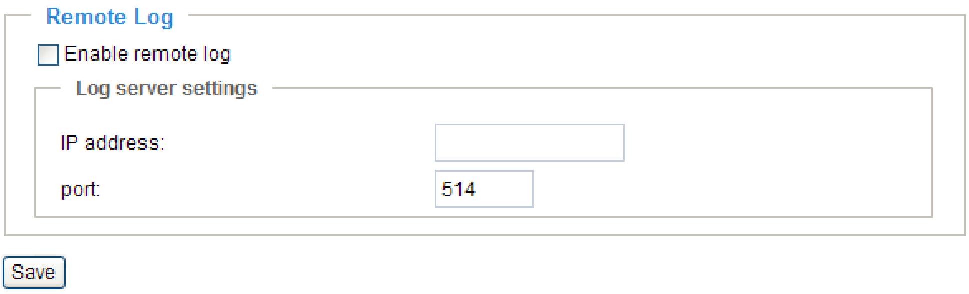
■ Click **NAS** **(Destination)**: Opens the file list of recordings as shown below. For more information about folder naming rule, please refer to page 77 for details.



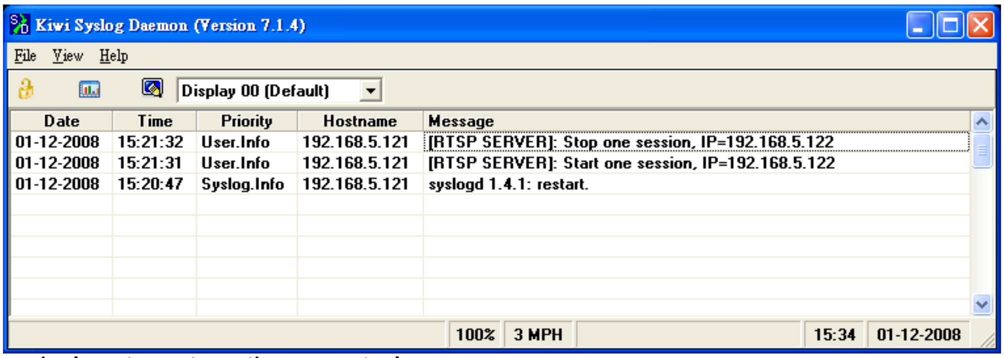
System Log Advanced Mode

This section explains how to configure the Network Camera to send the system log to the remote server as backup.

Remote Log



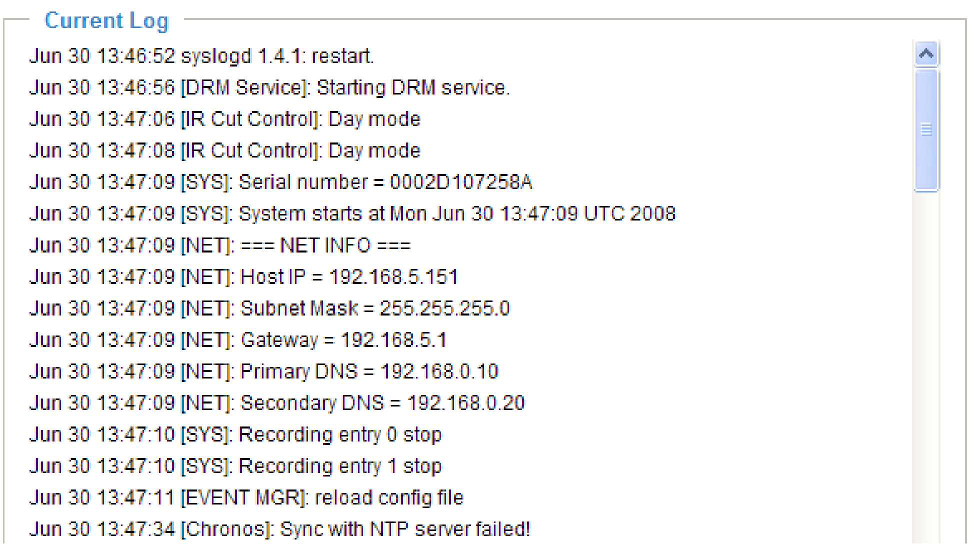
You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.



Follow the steps below to set up the remote log:

1. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, select **Enable remote log** and click **Save** to enable the setting.

Current Log



This column displays the system log in chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when reaching a maximum limit.

View Parameters Advanced Mode

The View Parameters page lists the entire system's parameters in alphabetical order. If you need technical assistance, please provide the information listed on this page.

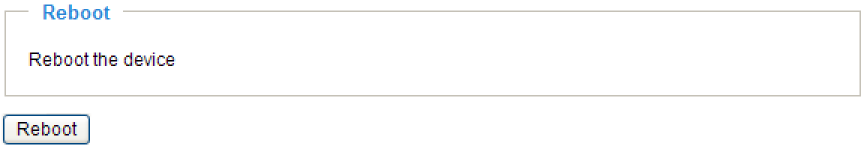
Parameter List

```
system_hostname='Wireless Network Camera'
system_ledoff='0'
system_date='2009/05/21'
system_time='16:40:01'
system_datetime='052116382009.08'
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-1
system_updateinterval='0'
system_info_modelname='PZ71x2'
system_info_extendedmodelname='PZ71x2'
system_info_serialnumber='0002D1778899'
system_info_firmwareversion='PZ71X2-VVTK-0102c'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
system_info_language_i5='日本語'
system_info_language_i6='Português'
system_info_language_i7='简体中文'
system_info_language_i8='繁體中文'
system_info_language_i9=''
system_info_language_i10=''
system_info_language_i11=''
system_info_language_i12=''
system_info_language_i13=''
system_info_language_i14=''
system_info_language_i15=''
system_info_language_i16=''
system_info_language_i17=''
```

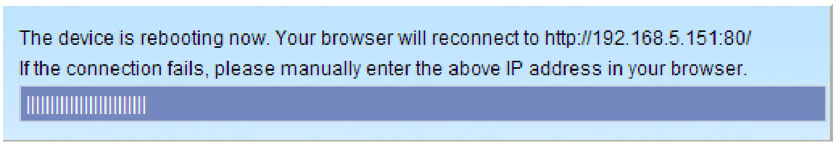
Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

Reboot

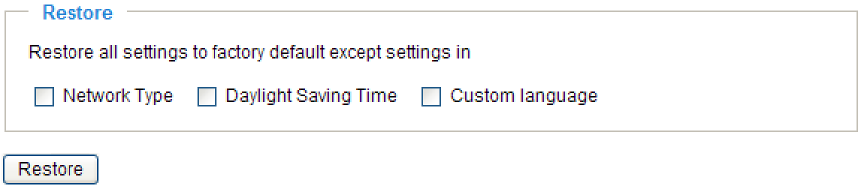


This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the rebooting process.



If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

Restore



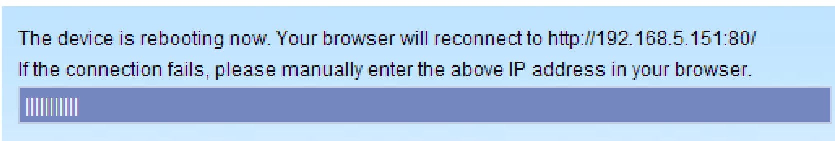
This feature allows you to restore the Network Camera to factory default settings.

Network Type: Select this option to retain the Network Type settings. (Please refer to Network Type on page 32.)

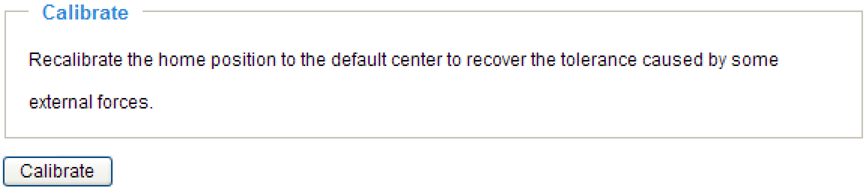
Daylight Saving Time: Select this option to retain the Daylight Saving Time settings. (Please refer to System on page 24.)

Custom Language: Select this option to retain the Custom Language settings.

If none of the options is selected, all settings will be restored to factory default.
The following message is displayed during the restoring process.



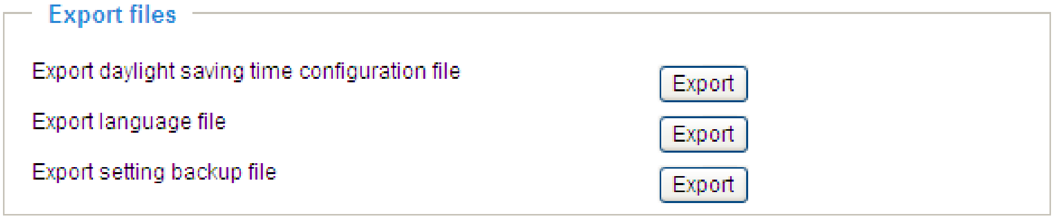
Calibrate



This feature re-calibrate the home position to the default center to recover the any displacement caused by external forces. Please note that there is no confirm message box after clicking on Calibrate, and the Network Camera will calibrate immediately.

Export / Upload Files Advanced Mode

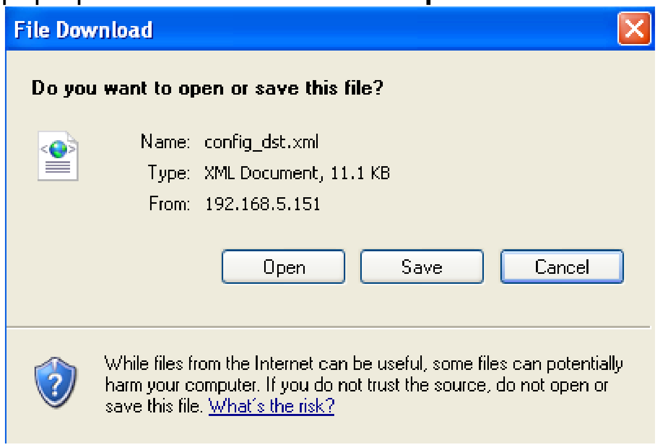
This feature allows you to Export / Upload daylight saving time rules, custom language files, and setting backup files.





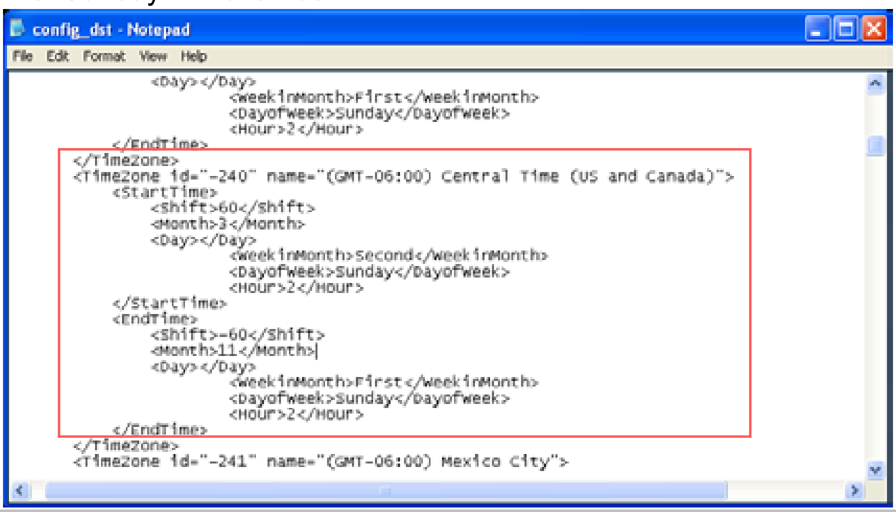
Export daylight saving time configuration file: Click to set the start and end time of DST.

Follow the steps below to export:
1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.



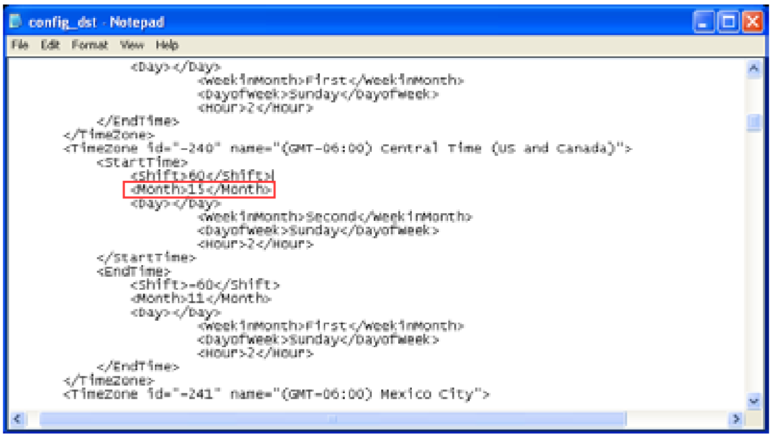
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



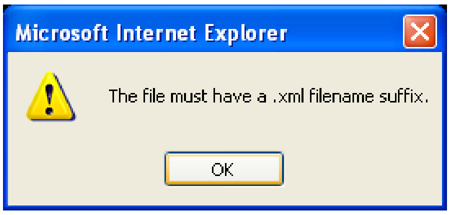
Upload daylight saving time rule: Click **Browse…** and specify the XML file to upload.

If the incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.





The following message is displayed when attempting to upload an incorrect file format.



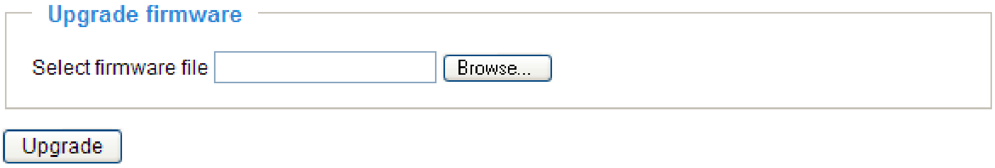
Export language file: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Upload custom language file: Click **Browse…** and specify your own custom language file to upload.

Export setting backup file: Click to export all parameters for the device and user-defined scripts.

Upload setting backup file: Click **Browse…** to upload a setting backup file. Please note that the model and firmware version of the device should be the same as the setting backup file. If you have set up a fixed IP or other special settings for your device, it is not suggested to upload a settings backup file.

Upgrade Firmware



This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.
Note: Do do not power off the Network Camera during the upgrade!

Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, re-access the Network Camera.

The following message is displayed when the upgrade has succeeded.

```
Reboot system now!!
This connection will close.
```

The following message is displayed when you have selected an incorrect firmware file.

```
Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is
completed.
This will take about 1 - 5 minutes.
Wrong PKG file format
Unpack fail
```

Appendix

URL Commands for the Network Camera

Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets should also be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced syntax as shown below. For example, name of the server is written as <servername> and is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam. adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data returned as HTTP formatted, i.e., starting with the string HTTP is line separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

http://<*servername*>/cgi-bin/<*subdir*>[/<*subdir*>...]/<*cgi*>.<*ext*>
[?<parameter>=<value>[&<parameter>=<value>...]]

Example: Set digital output #1 to active

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

Security Level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera. 2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator access rights can modify most of the camera's parameters except some privileges and network options.
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator access rights can fully control the camera's operations.
7	N/A	Internal parameters. Unable to be changed by any external interfaces.

Get Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/viewer/getparam.cgi?[<*parameter*>]
[&<parameter>…]

```
http://<servername>/cgi-bin/operator/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/admin/getparam.cgi?[<parameter>]
[&<parameter>…]
```

Where the <*parameter*> should be <*group*>[_<*name*>] or <*group*>[.<*name*>]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only <*group*>, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.

A successful control request returns parameter pairs as follows:

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

<length> is the actual length of content.

Example: Request IP address and its response

```
Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Set Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/setparam.cgi? <*parameter*>=<*value*> [&<parameter>=<value>…][&update=<value>][&return=<return page>] http://<*servername*>/cgi-bin/viewer/setparam.cgi? <*parameter*>=<*value*> [&<parameter>=<value>…][&update=<value>] [&return=<return page>] http://<*servername*>/cgi-bin/operator/setparam.cgi? <*parameter*>=<*value*> [&<parameter>=<value>…][&update=<value>] [&return=<return page>] http://<*servername*>/cgi-bin/admin/setparam.cgi? <*parameter*>=<*value*> [&<parameter>=<value>…][&update=<value>] [&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign <*value*> to the parameter <*group*>_<*name*>*.*
update	<boolean>	Set to 1 to update all fields (no need to update parameter in each group).
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned*.* The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (Note: The return page can be a general HTML file (.htm, .html) or a VIVOTEK server script executable (.vspx) file. It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list

Return:

HTTP/1.0 200 OK\r\n Content-Type: text/html\r\n Context-Length: <length>\r\n \r\n <*parameter pair*>

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and are readable will be returned.

Example: Set the IP address of server to 192.168.0.123:

Request:

http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

```
Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Available parameters on the server

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text strings shorter than ‘n’ characters. The characters “,’, <,>,& are invalid.
password[<n>]	The same as string but displays ‘*’ instead.
integer	Any number between $(-2^{31} – 1)$ and $(2^{31} – 1)$.
positive integer	Any number between 0 and $(2^{32} – 1)$.
<m> ~ <n>	Any number between ‘m’ and ‘n’.
domain name[<n>]	A string limited to a domain name shorter than ‘n’ characters (eg. www.ibm.com).
email address [<n>]	A string limited to an email address shorter than ‘n’ characters (eg. joe@www.ibm.com).
ip address	A string limited to an IP address (eg. 192.168.1.1).
mac address	A string limited to contain a MAC address without hyphens or colons.
boolean	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, …	Enumeration. Only given values are valid.
blank	A blank string.
everything inside <>	A description
positive Integer	Any number between 0 and $(2^{32} – 1)$
integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server.
text	SQLite data type. The value is a text string, stored using the database encoding (UTF-8, UTF-16BE or UTF-16-LE).
coordinate	x, y coordinate (eg. 0,0)
window size	window width and height (eg. 800x600)

NOTE: The camera should not be restarted when parameters are changed.

Group: system

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	1/6	Host name of server (Network Camera, Wireless Network Camera)
ledoff	<boolean>	6/6	Turn on (0) or turn off (1) all led indicators.
date	<yyyy/mm/dd>, keep, auto	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhhmmYYYY.ss>	6/6	Another current time format of the system.
ntp	<domain name>, <ip address>, <blank>	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-480 ~ 520	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -180: GMT-04:30 Caracas -160: GMT-04:00 Atlantic Time, Canada, La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Time: Dublin,

			Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean>	6/6	Enable automatic daylight saving time in time zone.
daylight_dstactualmode	<boolean>	6/7	Check if current time is under daylight saving time.
daylight_auto_begintime	string[19]	6/7	Display the current daylight saving start time. (product dependent)
daylight_auto_endtime	string[19]	6/7	Display the current daylight saving end time. (product dependent)

updateinterval	0, 3600, 86400, 604800, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive integer>	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptdst	<Any value>	7/6	Restore the system parameters to default values except all daylight saving time settings. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.
restoreexceptlang	<Any Value>	7/6	Restore the system parameters to default values except the custom language file the user has uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.

Subgroup of system: info (The fields in this group are unchangeable.)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	0/7	Internal model name of the server (eg. IP7139)
serialnumber	<mac address>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]	0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_count	<integer>	0/7	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16]	0/7	Available language lists.
customlanguage_maxcount	<integer>	0/7	Maximum number of custom languages supported on the server.

customlanguage_count	<integer>	0/7	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(maxcount-1)>	string	0/7	Custom language name.

Group: status

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
videomode_c0	ntsc, pal	4/7	The actual modulation type (videoin.type=0).
di_i<0~(ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
do_i<0~(ndo-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
onlinenum_rtsp	integer	6/7	Current number of RTSP connections.
onlinenum_httppush	integer	6/7	Current number of HTTP push server connections.
eth_i0	<string>	1/99	Get network information from mii-tool.

Group: di_i<0~(ndi-1)>

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	1/1	Indicates open circuit or closed circuit (inactive status)

Group: do_i<0~(ndo-1)>

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	1/1	Indicate open circuit or closed circuit (inactive status)

Group: security

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
privilege_do	view, operator, admin	6/6	Indicate which privileges and above can control digital output
privilege_camctrl	view, operator, admin	6/6	Indicate which privileges and above can control PTZ
user_i0_name	root	6/7	User name of root
user_i<1~20>_name	string[64]	6/7	User name
user_i0_pass	password[64]	6/6	Root password

user_i<1~20>_pass	password[64]	7/6	User password
user_i0_privilege	admin	6/7	Root privilege
user_i<1~20>_ privilege	viewer, operator, admin	6/6	User privilege

Group: network

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
type	lan, pppoe	6/6	Network connection type.
resetip	<boolean>	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.
ipaddress	<ip address>	6/6	IP address of server.
subnet	<ip address>	6/6	Subnet mask.
router	<ip address>	6/6	Default gateway.
dns1	<ip address>	6/6	Primary DNS server.
dns2	<ip address>	6/6	Secondary DNS server.
wins1	<ip address>	6/6	Primary WINS server.
wins2	<ip address>	6/6	Secondary WINS server.

Subgroup of network: ipv6

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable IPv6.
addonipaddress	<ip address>	6/6	IPv6 IP address.
addonprefixlen	0~128	6/6	IPv6 prefix length.
addonrouter	<ip address>	6/6	IPv6 router address.
addondns	<ip address>	6/6	IPv6 DNS address.
allowoptional	<boolean>	6/6	Allow manually setup of IP address setting.

Subgroup of network: ftp

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	6/6	Local ftp server port.

Subgroup of network: http

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	6/6	HTTP port.
alternateport	1025~65535	6/6	Alternate HTTP port.
authmode	basic, digest	1/6	HTTP authentication mode.
s0_accessname	string[32]	1/6	HTTP server push access name for stream 1.
s1_accessname	string[32]	1/6	HTTP server push access name for stream 2.
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.

Subgroup of network: https

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	6/6	HTTPS port.

Subgroup of network: rtsp

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	1/6	RTSP port.
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	1/6	RTSP authentication mode.
s0_accessname	string[3b;42]	1/6	RTSP access name for stream1.
s1_accessname	string[32]	1/6	RTSP access name for stream2.
s0_audiotrack	<integer>	6/6	The current audio track for stream1. -1 => audio mute
s1_audiotrack	<integer>	6/6	The current audio track for stream2. -1 => audio mute

Subgroup of network_rtsp_s<0~(n-1)>: multicast, n is stream count

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	4/4	Enable always multicast.
ipaddress	<ip address>	4/4	Multicast IP address.
videoport	1025 ~ 65535	4/4	Multicast video port.
audioport	1025 ~ 65535	4/4	Multicast audio port.
ttl	1 ~ 255	4/4	Mutlicast time to live value.

Subgroup of network: sip

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	6/6	SIP port. (capability.protocol.sip=1)

Subgroup of network: rtp

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	6/6	Video channel port for RTP. (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	6/6	Audio channel port for RTP. (capability.protocol.rtp_unicast=1)

Subgroup of network: pppoe

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
user	string[128]	6/6	PPPoE account user name.
pass	password[64]	6/6	PPPoE account password.

Group: wireless (only in PZ71x2)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
ssid	string[32]	6/6	SSID for wireless lan settings. The valid characters are [A-Z] [a-z] [0-9] [/] [.] [_] [=] [ ] [-] [+] [*].
wlmode	Infra, Adhoc	6/6	Wireless mode. Infra: Infrastructure
channel	1~11 or 1 ~ 13 or 10~11 or 10~13 or 1~14	6/6	USA and Canada Europe Spain France All
txrate	0 ~ 12	6/6	0 -> Auto 1 -> 1Mbps 2 -> 2Mbps 3 -> 5.5Mbps 4 -> 11Mbps 5 -> 6Mbps 6 -> 9Mbps

			7 -> 12Mbps 8 -> 18Mbps 9 -> 24Mbps 10 -> 36Mbps 11 -> 48Mbps 12 -> 54Mbps
encrypt	0~3	6/6	Encryption method (product dependent): 0=> NONE, 1 => WEP, 2 => WPA, 3 => WPA2PSK
authmode	OPEN, SHARED	6/6	Authentication mode.
keylength	64, 128	6/6	Key length in bits.
keyformat	HEX, ASCII	6/6	Key1 ~ key4 presentation format.
keyselect	1 ~ 4	6/6	Default key number.
key1	password [32]	6/6	WEP key1 for encryption. The valid characters are [A-Z] [a-z] [0-9].
key2	password [32]	6/6	WEP key2 for encryption. The valid characters are [A-Z] [a-z] [0-9].
key3	password [32]	6/6	WEP key3 for encryption. The valid characters are [A-Z] [a-z] [0-9].
key4	password [32]	6/6	WEP key4 for encryption. The valid characters are [A-Z] [a-z] [0-9].
domain	'U' for USA 'C' for Canada 'E' for Euro 'S' for Spain 'F' for France 'I' for Isrel 'A' for All	6/7	Wireless domain.
algorithm	AES, TKIP	6/6	Algorithm
presharedkey	password [63]	6/6	WPA mode pre-shared key. The valid characters are [A-Z] [a-z] [0-9].

Group: ipfilter

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable access list filtering.
admin_enable	<boolean>	6/6	Enable administrator IP address.

admin_ip	String[44]	6/6	Administrator IP address.
maxconnection	1~10	6/6	Maximum number of concurrent streaming connection(s).
allow_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Allowed starting IPv4 address for connection.
allow_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Allowed ending IPv4 address for connection.
deny_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Denied starting IPv4 address for connection.
deny_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Denied ending IPv4 address for connection.
ipv6_allow_i<0~9>	String[44]	6/6	Allowed IPv6 address for connection.
ipv6_deny_i<0~9>	String[44]	6/6	Denied IPv6 address for connection.

Group: videoin_c<0~(n-1)> for n channel products, m is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
whitebalancemode	0~1	4/4	0: auto tracking white balance 1: white balance control
autotrackingwhitebalance	0~8	4/4	Adjust colors by setting different levels. Set videoin_c0_whitebalancemode to 0 before setting this parameter.
whitebalancecontrol	0~8	4/4	Set different levels to meet different color temperatures (3200K~9600K). Set whitebalancemode to 1 before setting this parameter.
irislevel	1 ~ 8	4/4	Iris level when connect to auto iris lens. 8 => most brightness, 1 => most darkness
autoiris	0~1	4/4	set 1 to enable auto iris, set 0 to disable auto iris
autoelectronicshutter	0~7	4/4	Set electronica shutter speed. Set 0 for auto shutter, set 1 for fixed at 1/60 (1/50). Bigger value, faster shutter.
enableblc	0~1	4/4	Enable backlight compensation
lowluxmode	0~1	4/4	Turn off or on low lux mode
obwlowluxmode	0~1	4/4	Turn on or off black/white video in low lux mode
blcarea_i<0~5>	0~7	4/4	Set back light compensation level
blcsenslevel	0~7	4/4	Set back light compensation level

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
color	0, 1	4/4	0 =>monochrome 1 => color
flip	<boolean>	4/4	flip the image
mirror	<boolean>	4/4	mirror the image
text	string[16]	1/4	enclosed caption
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video
s<0~(m-1)>_codectype	mpeg4, mjpeg	4/4	video codec type
s<0~(m-1)>_resolution	QCIF, (176x120,ntsc) (176x144,pal) CIF, (352x240,ntsc) (352x288,pal) 4CIF, (704x480,ntsc) (704x576,pal)	4/4	Video resolution in pixel
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	4/4	The period of intra frame in milliseconds
s<0~(m-1)>_mpeg4_ratecontrolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	0~5	4/4	quality of video when choosing vbr in "ratecontrolmode". 0 is customized manual input setting. 1 is worst quality and 5 is the best quality.
s<0~(m-1)>_mpeg4_quantlevel	1~31	4/4	The specific quality parameter of the Mpeg4 encoder. 1 = best quality, 31 = worst quality.
s<0~(m-1)>_mpeg4_bitrate	1000~4000000	4/4	Set bit rate in bps when choose cbr in "ratecontrolmode"
s<0~(m-1)>_mpeg4_maxframe	1~25, 26~30 (only for NTSC)	4/4	set maximum frame rate in fps (for MPEG-4)
s<0~(m-1)>_mjpeg_quant	0 ~ 5	4/4	quality of jpeg video. 0 is customized manual input setting. 1 is worst quality and 5 is the best quality.

s<0~(m-1)>_mjpeg_quantlevel	10~200	4/4	The specific quality parameter of the JPEG encoder. 10 = best quality, 200 = worst quality.
s<0~(m-1)>_mjpeg_maxframe	1~25, 26~30 (only for NTSC)	4/4	set maximum frame rate in fps (for JPEG)

Group: audioin_c<0~(n-1)> for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
mute	0, 1	4/4	Enable audio mute.
gain	0~45	4/4	Gain of line input
gain2	0~45	4/4	Gain of external microphone input
s<0~(m-1)>_codectype	aac4, gamr	4/4	Set audio codec type for input.
s<0~(m-1)>_aac4_bitrate	16000, 32000, 48000, 64000, 96000, 128000	4/4	Set AAC4 bitrate in bps.
s<0~(m-1)>_gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	4/4	Set AMR bitrate in bps.

Group: image_c<0~(n-1)> for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5	4/4	Adjust brightness of image according to mode settings.
saturation	-5 ~ 5	4/4	Adjust saturation of image according to mode settings.
contrast	-5 ~ 5	4/4	Adjust contrast of image according to mode settings.
sharpness	-3 ~ 3	4/4	Adjust sharpness of image according to mode settings.

Group: timeshift, c for n channel products, m is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable time shift streaming.
c<0~(n-1)>_s<0~(m-1)>_allow	<boolean>	4/4	Enable time shift streaming for specific stream.

Group: motion_c<0~(n-1)> for m profile and n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean>	4/4	Enable motion window 1~3.
win_i<0~2>_name	string[14]	4/4	Name of motion window 1~3.
win_i<0~2>_left	0 ~ 320	4/4	Left coordinate of window position.
win_i<0~2>_top	0 ~ 240	4/4	Top coordinate of window position.
win_i<0~2>_width	0 ~ 320	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	4/4	Sensitivity of motion detection window.

Group: ddns

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the dynamic DNS.
provider	Safe100, DyndnsDynamic, DyndnsCustom, TZO, DHS, DynInterfree, CustomSafe100	6/6	Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom) TZO => tzo.com DHS => dhs.org DynInterfree =>dyn-interfree.it CustomSafe100 => Custom server using safe100 method
<provider>_hostname	string[128]	6/6	Your dynamic hostname.
<provider>_username email	string[64]	6/6	Your user or email to login to the DDNS service provider
<provider>_password key	string[64]	6/6	Your password or key to login to the DDNS service provider.
<provider>_serverna me	string[128]	6/6	The server name for safe100. (This field only exists if the provider is customsafe100)

Group: upnppresentation

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP presentation service.

Group: upnpportforwarding

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP port forwarding service.
upnpnatstatus	0~3	6/7	The status of UpnP port forwarding, used internally. 0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding

Group: syslog

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	6/6	Enable remote log.
serverip	<IP address>	6/6	Log server IP address.
serverport	514, 1025~65535	6/6	Server port used for log.
level	0~7	6/6	Levels used to distinguish the importance of the information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

Group: camctrl_c<0~(n-1)> for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	1/4	Pan speed
tiltspeed	-5 ~ 5	1/4	Tilt speed
zoomspeed	-5 ~ 5	1/4	Zoom speed
autospeed	1 ~ 5	1/4	Auto pan speed
focusspeed	-5 ~ 5	1/4	Auto focus speed
axisx	-6790 ~ 6790	1/7	Axis X coordinate, used internally.

axisy	-786 ~ 1572	1/7	Axis Y coordinate, used internally.
axisz	4096 ~ 8859	1/7	Axis Z coordinate, used internally.
returnhome	0,1	1/4	Enable/disable auto return home while idle
returnhomeinterval	1 ~ 999	1/4	Wait interval return home
defaulthome	0,1	1/4	This field tells system to use default home position or not.
osdzoom	0,1	1/4	Enable zoom times display
digitalzoom	0,1	1/4	Enable digital zoom
preset_i<0~19>_name	string[40]	1/4	Name of the preset location.
preset_i<0~19>_pan	-6790 ~ 6790	1/4	The axis x coordinate of each preset location
preset_i<0~19>_tilt	-786 ~ 1572	1/4	The axis y coordinate of each preset location
preset_i<0~19>_zoom	4096 ~ 8859	1/4	The axis z coordinate of each preset location
patrol_i<0~39>_name	string[40]	1/4	The name of patrol location
patrol_i<0~39>_ dwelling	0 ~ 999	1/4	The dwelling time of each patrol location

Group: layout

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1/6	0 => Custom logo 1 => Default logo
logo_link	string[40]	1/6	Hyperlink of the logo
logo_powerbyvvtk_hidden	<boolean>	1/6	Hide Powered by VIVOTEK
theme_option	1~4	1/6	1~3: One of the default themes. 4: Custom definition.
theme_color_font	string[7]	1/6	Font color
theme_color_configfont	string[7]	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	1/6	Font color of video title.
theme_color_controlbackground	string[7]	1/6	Background color of control area.
theme_color_configbackground	string[7]	1/6	Background color of configuration area.
theme_color_videobackground	string[7]	1/6	Background color of video area.
theme_color_case	string[7]	1/6	Frame color

Group: capability

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
api_httpversion	0100a	0/7	The HTTP API version.
bootuptime	<positive integer>	0/7	Server bootup time.
nir	0,	0/7	Number of IR interfaces.

	<positive integer>		
npir	0, <positive integer>	0/7	Number of PIRs.
ndi	0, <positive integer>	0/7	Number of digital inputs.
ndo	0, <positive integer>	0/7	Number of digital outputs.
naudioin	0, <positive integer>	0/7	Number of audio inputs.
naudioout	0, <positive integer>	0/7	Number of audio outputs.
nvideoin	<positive integer>	0/7	Number of video inputs.
nmediastream	<positive integer>	0/7	Number of media stream per channels.
nvideosetting	<positive integer>	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	0/7	Number of UART interfaces.
ptzenabled	<positive integer>	0/7	An 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => Built-in or external camera; 0(external), 1(built-in) Bit 2 => Support pan operation, 0(not support), 1(support) Bit 3 => Support tilt operation; 0(not support), 1(support) Bit 4 => Support zoom operation; 0(not support), 1(support) Bit 5 => Support focus operation; 0(not support), 1(support) Bit 6 => Support iris operation; 0(not support), 1(support) Bit 7 => External or built-in PT; 0(built-in), 1(external) Bit 8 => Invalidate bit 1 ~ 7; 0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid) Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid),

			1(fields are invalid)
lens_pan	<positive integer>	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support pan. Bit 1 => Support pan in UI. Bit 2 => External or built-in pan function; 0(built-in), 1(external).
lens_tilt	<positive integer>	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support tilt. Bit 1 => Support tilt in UI. Bit 2 => External or built-in tilt function; 0(built-in), 1(external).
lens_zoom	<positive integer>	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support zoom Bit 1 => Support zoom in UI Bit 2 => External or built-in zoom function; 0(built-in), 1(external).
lens_focus	<positive integer>	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support focus. Bit 1 => Support focus in UI. Bit 2 => External or built-in focus function; 0(built-in), 1(external). Bit 3 => Support auto focus in UI.
lens_iris	<positive integer>	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support iris. Bit 1 => Support iris in UI. Bit 2 => External or build-in iris function; 0(build-in), 1(external). Bit 3 => Support auto iris in UI.
npreset	<positive integer>	0/7	Number of preset locations.
protocol_https	< boolean >	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	0/7	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	0/7	The maximum allowed simultaneous connections.
protocol_maxgenconnection	<positive integer>	0/7	The maximum general streaming connections .

protocol_maxmegaconnection	<positive integer>	0/7	The maximum megapixel streaming connections.
protocol_rtp_multicast_scalable	<boolean>	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multicast_backchannel	<boolean>	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mjpeg	<boolean>	0/7	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	0/7	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	0/7	Indicate whether to support IPv6.
videoin_type	0, 1, 2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of available resolution separated by commas>	0/7	Available resolutions list.
videoin_maxframerate	<a list of available maximum frame rate separated by commas>	0/7	Available maximum frame list.
videoin_codec	<a list of available codec types separated by commas>	0/7	Available codec list.
videoout_codec	<a list of the available codec types separated by commas)	0/7	Available codec list.
audio_aec	<boolean>	0/7	Indicate whether to support acoustic echo cancellation.
audio_extmic	<boolean>	0/7	Indicate whether to support external microphone input.
audio_linein	<boolean>	0/7	Indicate whether to support external line input.
audio_lineout	<boolean>	0/7	Indicate whether to support line output.
audio_headphoneout	<boolean>	0/7	Indicate whether to support headphone output.
audioin_codec	<a list of the available codec types separated by commas)	0/7	Available codec list.

audioout_codec	<a list of the available codec types separated by commas)	0/7	Available codec list.
uart_httptunnel	<boolean>	0/7	Indicate whether to support HTTP tunnel for UART transfer.
camctrl_privilege	<boolean>	0/7	Indicate whether to support “Manage Privilege” of PTZ control in the Security page.
transmission_mode	Tx, Rx, Both	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	0/7	Indicate whether to support wireless.
wireless_802dot11b	<boolean>	0/7	Indicate whether to support wireless 802.11b+.
wireless_802dot11g	<boolean>	0/7	Indicate whether to support wireless 802.11g.
wireless_beginchannel	1 ~ 14	0/7	Indicate the begin channel of wireless network
wireless_endchannel	1 ~ 14	0/7	Indicate the end channel of wireless network
wireless_encrypt_wep	<boolean>	0/7	Indicate whether to support wireless WEP.
wireless_encrypt_wpa	<boolean>	0/7	Indicate whether to support wireless WPA.
wireless_encrypt_wpa2	<boolean>	0/7	Indicate whether to support wireless WPA2.
derivative_brand	<boolean>	0/7	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
evctrlchannel	<boolean>	0/7	Indicate whether to support HTTP tunnel for event/control transfer.
joystick	<boolean>	0/7	Indicate whether to support joystick control.

Group: event_customtaskfile_i<0~2>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[41]	6/6	Custom script identification of this entry.
date	string[17]	6/6	Date of custom script.
time	string[17]	6/6	Time of custom script.

Group: event_i<0~2>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry.

enable	0, 1	6/6	Enable or disable this event.
priority	0, 1, 2	6/6	Indicate the priority of this event: "0" = low priority "1" = normal priority "2" = high priority
delay	1~999	6/6	Delay in seconds before detecting the next event.
trigger	boot, di, motion, seq, recnotify,	6/6	Indicate the trigger condition: "boot" = System boot "di"= Digital input "motion" = Video motion detection "seq" = Periodic condition "recnotify" = Recording notification.
di	<integer>	6/6	Indicate which DI detects. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.
mdwin	<integer>	6/6	Indicate which motion detection windows detect. This field is required when trigger condition is "md". One bit represents one window. The LSB indicates the 1^{st} window. For example, to detect the 1^{st} and 3^{rd} windows, set mdwin as 5.
inter	1~999	6/6	Interval of snapshots in minutes. This field is used when trigger condition is "seq".
weekday	<integer>	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	6/6	Begin time of the weekly schedule.
endtime	hh:mm	6/6	End time of the weekly schedule. (00:00 ~ 24:00 sets schedule as always on)
action_do_i<0~(ndo-1)>_enable	0, 1	6/6	Enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	6/6	Duration of the digital output trigger in seconds.

action_goto_enable	0,1	6/6	Enable/disable ptz goto preset on event triggered.
action_goto_name	string[40]	6/6	Preset name that ptz goto on event triggered.
action_server_i<0~4>_enable	0, 1	6/6	Enable or disable this server action. The default value is 0.
action_server_i<0~4>_media	NULL, 0~4	6/6	Index of the attached media.
action_server_i<0~4>_datefolder	<boolean>	6/6	Enable this to create folders by date, time, and hour automatically.

Group: server_i<0~4>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry
type	email, ftp, http, ns	6/6	Indicate the server type: "email" = email server "ftp" = FTP server "http" = HTTP server "ns" = network storage
http_url	string[128]	6/6	URL of the HTTP server to upload.
http_username	string[64]	6/6	Username to log in to the server.
http_passwd	string[64]	6/6	Password of the user.
ftp_address	string[128]	6/6	FTP server address.
ftp_username	string[64]	6/6	Username to log in to the server.
ftp_passwd	string[64]	6/6	Password of the user.
ftp_port	0~65535	6/6	Port to connect to the server.
ftp_location	string[128]	6/6	Location to upload or store the media.
ftp_passive	0, 1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	6/6	Email server address.
email_sslmode	0, 1	6/6	Enable support SSL.
email_port	0~65535	6/6	Port to connect to the server.
email_username	string[64]	6/6	Username to log in to the server.
email_passwd	string[64]	6/6	Password of the user.
email_senderemail	string[128]	6/6	Email address of the sender.
email_recipientemail	string[128]	6/6	Email address of the recipient.
ns_location	string[128]	6/6	Location to upload or store the media.
ns_username	string[64]	6/6	Username to log in to the server.
ns_passwd	string[64]	6/6	Password of the user.
ns_workgroup	string[64]	6/6	Workgroup for network storage.

Group: media_i<0~4> (media_freespace is used internally.)

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry
type	snapshot, systemlog, videoclip, recordmsg	6/6	Media type to send to the server or store on the server.
snapshot_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
snapshot_prefix	string[16]	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	6/6	The number of post-event images.
videoclip_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
videoclip_prefix	string[16]	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	6/6	Indicates the time for pre-event recording in seconds.
videoclip_maxduration	1 ~ 10	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 1500	6/6	Maximum size of one video clip file in Kbytes.

Group: recording_i<0~1>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry.
enable	0, 1	6/6	Enable or disable this recording.
priority	0, 1, 2	6/6	Indicate the priority of this recording: “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.
source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc.
limitsize	0,1	6/6	0: Entire free space mechanism 1: Limit recording size mechanism

cyclic	0,1	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	6/6	0: Disable recording notification 1: Enable recording notification
notifyserver	0~31	6/6	Indicate which notification server is scheduled. One bit represents one application server (server_i0~i4). bit0 (LSB) = server_i0. bit1 = server_i1. bit2 = server_i2. bit3 = server_i3. bit4 = server_i4. For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21.
weekday	<interger>	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	6/6	Start time of the weekly schedule.
endtime	hh:mm	6/6	End time of the weekly schedule. (00:00~24:00 indicates schedule always on)
prefix	string[16]	6/6	Indicate the prefix of the filename.
cyclesize	20~	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.
reserveamount	15~	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.
dest	cf, 0~4	6/6	The destination to store the recorded data. “0~4” means the index of the network storage.

Group: path

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
encoder1_start	<boolean>	7/7	Specify the HTTP push server is active for stream 1
encoder2_start	<boolean>	7/7	Specify the HTTP push server is active for stream 2

Group: https

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
connect	1025 ~ 65535	7/7	Specify the stunnel connect port.
enable	<boolean>	6/6	To enable or disable secure HTTP.
policy	<Boolean>	6/6	If the value is 1, it will force HTTP connection redirect to HTTPS connection
method	auto, manual, install	6/6	auto => Create self-signed certificate automatically. manual => Create self-signed certificate manually. install => Create certificate request and install.
status	-2 ~ 1	6/6	Specify the https status. -2= Invalid public key -1 = Waiting for certificate 0 = Not installed 1= Active
countryname	string[2]	6/6	Country name in the certificate information.
stateorprovincename	string[128]	6/6	State or province name in the certificate information.
localityname	string[128]	6/6	The locality name in the certificate information.
organizationname	string[64]	6/6	Organization name in the certificate information.
unit	string[32]	6/6	Organizational unit name in the certificate information.
commonname	string[64]	6/6	Common name in the certificate information.
validdays	0 ~ 9999	6/6	Valid period for the certification.

Drive the digital output

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/setdo.cgi?do1=<*state*>[&do2=<state>]
[&do3=<state>][&do4=<state>][&return=<*return page*>]

Where state is 0 or 1; “0” means inactive or normal state, while “1” means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state

return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Example: Drive the digital output 1 to triggered state and redirect to an empty page.

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

Query Status of the Digital Input

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]

If no parameter is specified, all of the digital input statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[di0=<state>]\r\n
[di1=<state>]\r\n
[di2=<state>]\r\n
[di3=<state>]\r\n
```

where *<state>* can be 0 or 1.

Example: Query the status of digital input 1 .

Request:

http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di1=1\r\n
```

Query Status of the Digital Output

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]

If no parameter is specified, all the digital output statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[do0=<state>]\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
[do3=<state>]\r\n
```

where <*state*> can be 0 or 1.

Example: Query the status of digital output 1.

Request:

http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
do1=1\r\n
```

Capture Single Snapshot

Note: This request requires Normal User privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>] [&quality=<value>]

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	The channel number of the video source.
resolution	*<available resolution>*	0	The resolution of the image.
quality	*1~5*	3	The quality of the image.

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

Return:

HTTP/1.0 200 OK\r\n *Content-Type: image/jpeg\r\n* *[Content-Length: <image size>\r\n]* *<binary JPEG image data>*

Account Management

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/editaccount.cgi? method=<value>&username=<*name*>[&userpass=<*value*>][&privilege=<*value*>] [&privilege=<value>][…][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the "username" field is necessary. It will use the default value of other fields if not specified.
	Delete	Remove an account from the server. When using this method, the "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, the "username" field is necessary, and other fields are optional. If not specified, it will keep the original settings.

username	<name>	The name of the user to add, delete, or edit.
userpass	<value>	The password of the new user to add or that of the old user to modify. The default value is an empty string.
privilege	<value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.
	operator	Operator privilege.
	admin	Administrator privilege.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

System Logs

Note: This request require Administrator privileges.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/admin/syslog.cgi

Server will return the most up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

Upgrade Firmware

Note: This request requires Administrator privileges.

Method: POST

Syntax:

http://*<servername>*/cgi-bin/admin/upgrade.cgi

Post data:

```
fimage=<file name>[&return=<return page>]\r\n
```

\r\n <multipart encoded form data>

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

Camera Control

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/camctrl.cgi?[channel=<value>][&camid=<value>] { [&move=<value>] or [&focus=<value>] or [&iris=<value>] or [&speedpan=<value>] or [&speedtilt=<value>] or [&speedzoom=<value>] or [&speedapp=<value>] or [&auto=<value>] or [&zoom=<value>] or [&zooming=<value>] or [&vx=<value>&vy=<value>&vs=<value>] } [&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
camid	0,<positive integer>	Camera ID.
move	home	Move to camera to home position.
	up	Move camera up.
	down	Move camera down.
	left	Move camera left.
	right	Move camera right.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedapp	1 ~ 5	Set the auto pan/patrol speed.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop camera.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
	stop	Stop zoom.
zooming	wide	Zoom without stopping for larger view with current speed.
	tele	Zoom without stopping for further view with current speed.
vx	<integer , excluding 0>	The slope of movement = vy/vx, used for joystick control.
vy	<integer>	

vs	0 ~ 7	Set the speed of movement, "0" means stop.
focus	auto	Auto focus.
	far	Focus on further distance.
	near	Focus on closer distance.
iris	auto	Let the Network Camera control iris size.
	open	Manually control the iris for bigger size.
	close	Manually control the iris for smaller size.
sethome	define	Set current position as home position
	default	Using default home position
calibrate	go	Recalibrate the home position to the default center
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Recall

Note: This request requires Viewer privileges.

Method: GET

Syntax:

http://<*servername*>/cgi-bin/camctrl/recall.cgi?
recall=<value>[&channel=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
recall	Text string less than 30 characters	One of the present positions to recall.
channel	<0~(n-1)>	Channel of the video source.
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Preset Locations

Note: This request requires Operator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/preset.cgi?[channel=<value>]

[&addpos=<value>][&delpos=<value>][&return=*<return page>*]

PARAMETER	VALUE	DESCRIPTION
addpos	<Text string less than 30 characters>	Add one preset location to the preset list.
channel	<0~(n-1)>	Channel of the video source.
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

System Information

Note: This request requires Normal User privileges.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/sysinfo.cgi

Server will return the system information. In HTTP API version 2, the CapVersion will be 0200. All fields in the previous version (0100) are obsolete. Please use "getparam.cgi?capability" instead.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
Model=<model name of server>\r\n
CapVersion=0200\r\n
```

PARAMETER(supported capability version)	VALUE	DESCRIPTION
Model	system.firmwareversion	Model name of the server. Ex:IP3133-VVTK-0100a
CapVersion	*MMmm, MM is major version from 00 ~ 99* *mm is minor version from 00 ~ 99* *ex: 0100*	Capability field version.

IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<*ipaddress*>&end=<*ipaddress*>][&index=<*value*>]
[&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
Method	addallow	Add allowed IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	adddeny	Add denied IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	deleteallow	Remove allowed IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove denied IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The starting IP address to add or to delete.
end	<ip address>	The ending IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Get SDP of Streams

Note: This request requires Viewer access privileges.

Method: GET/POST

Syntax:

http://<*servername*>/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

"network_accessname_<0~(m-1)>" is the accessname for stream "1" to stream "m". Please refer to the "subgroup of network: rtsp" for setting the accessname of SDP.

You can get the SDP by HTTP GET.

Open the Network Stream

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

http://<*servername*>/<network_http_s<0~m-1>_accessname>

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player.

rtsp://<*servername*>/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

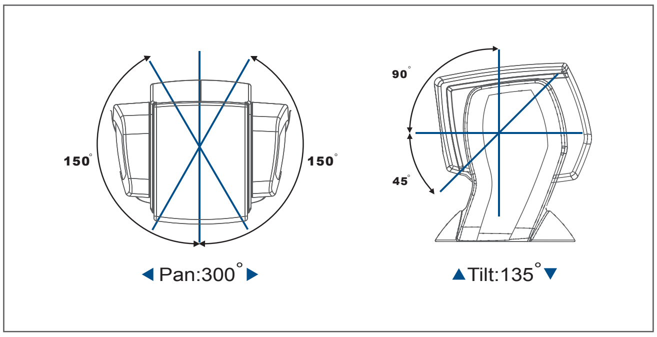
For details on streaming protocol, please refer to the "control signaling" and "data format" documents.

Technical Specifications

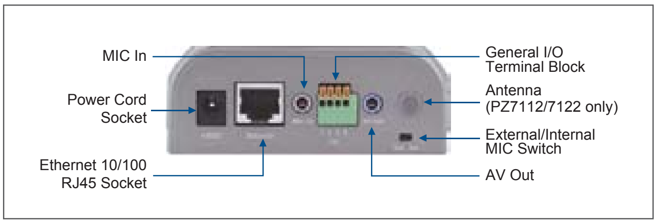
Models	· PZ7111 (NTSC CCD, PoE) · PZ7121 (PAL CCD, PoE) · PZ7112 (NTSC CCD, WLAN) · PZ7122 (PAL CCD, WLAN)
System	· CPU: Bach SoC · Flash: 8MB · RAM: 64MB + 32MB · Embedded OS: Linux 2.6
Pan/Tilt/Zoom	· Pan range: 300° (-150° ~ +150°) · Tilt range: 135° (-45° ~ +90°) · 10x optical zoom, 10x digital zoom · Auto pan mode · Auto patrol mode
Lens	· 10x optical zoom lens, f = 4.2 ~ 42 mm, F1.8 (wide), F2.9 (tele), auto-iris, auto focus
Angle of View	· 4.9° ~ 46° (horizontal) · 3.6° ~ 35° (vertical)
Shutter Time	· 1/60 sec. to 1/10,000 sec. (PZ7111/PZ7112) · 1/50 sec. to 1/10,000 sec. (PZ7121/PZ7122)
Image Sensor	· 1/4" CCD sensor in D1 resolution
Minimum Illumination	· 1.5 Lux / F1.8 (typical) · 0.05 Lux / F1.8 (low light mode)
Video	· Compression: MJPEG & MPEG-4 · Streaming: Simultaneous dual streams MPEG-4 streaming over UDP, TCP, HTTP or HTTPS MPEG-4 multicast streaming MJPEG streaming over HTTP or HTTPS · Supports 3GPP mobile surveillance · Frame rates: MPEG-4: Up to 30/25 fps at 704x480/704x576 MJPEG: Up to 30/25 fps at 704x480/704x576 · Interface: AV output
Image Settings	· Adjustable image size, quality and bit rate · Time stamp and text caption overlay · Flip & mirror · Configurable brightness, contrast, saturation, sharpness and white balance · ATW/AWB, AES/ALC · BLC (Backlight Compensation)
Audio	· Compression: GSM-AMR speech encoding, bit rate: 4.75 kbps to 12.2 kbps MPEG-4 AAC audio encoding, bit rate: 16 kbps to 128 kbps · Interface: Built-in microphone External microphone input Audio output External/Internal microphone switch · Supports two-way audio via SIP protocol · Supports audio mute
Networking	· 10/100 Mbps Ethernet, RJ-45 · Built-in 802.11b/g WLAN (PZ7112/PZ7122) · Protocols: IPv4, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS and PPPoE
Alarm and Event Management	· Triple-window video for motion detection · One D/I and one D/O for external sensor and alarm · Event notification using HTTP, SMTP or FTP · Local recording of MP4 files
Security	· Multi-level user access with password protection · IP address filtering · Wireless: WEP, WPA-PSK, WPA2 (PZ7112/PZ7122) · HTTPS encrypted data transmission
Users	· Live viewing for up to 10 clients
Dimension	· Ø 105 mm x 120 mm
Weight	· Net: 391 g (PZ7111/PZ7121) · Net: 408 g (PZ7112/PZ7122)

LED Indicator	· System power and status indicator · System activity and network link indicator
Power	· 12V DC · Power consumption: Max. 12 W (PZ7111/7121) · Power consumption: Max. 13 W (PZ7112/7122) · 802.3af compliant Power-over-Ethernet (PZ7111/PZ7121)
Approvals	· CE, LVD, FCC, VCCI, C-Tick
Operating Environments	· Temperature: 0 ~ 50 °C (32 ~ 122 °F) · Humidity: 20% ~ 80% RH
Viewing System Requirements	· OS: Microsoft Windows 2000/XP/Vista · Browser: Mozilla Firefox, Internet Explorer 6.x or above · Cell phone: 3GPP player · Real Player: 10.5 or above · Quick Time: 6.5 or above
Installation, Management, and Maintenance	· Installation Wizard 2 · 16-CH recording software · Supports firmware upgrade
Applications	· SDK available for application development and system integration
Warranty	· 24 months

Pan/Tilt Range



External View



Accessories



Enclosure



Mounting Kit

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE, OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

■ This device may not cause harmful interference, and

■ This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

■ Reorient or relocate the receiving antenna.

■ Increase the separation between the equipment and receiver.

■ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

■ Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

CE Mark Warning CE

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This device (PZ7112/PZ7122) complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC.

This device (PZ7112/PZ7122) is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device (PZ7112/PZ7122) may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.